NetIQ® AppManager® for Nortel™ Communication Server 2000/2100

Management Guide

February 2011

Legal Notice

Contents

About this Book and the Library

The NetIQ AppManager for Nortel CS2x product (AppManager) is a comprehensive solution for managing, diagnosing, and analyzing performance, availability, and health for a broad spectrum of operating environments, applications, services, and server hardware.

AppManager for Nortel CS2x provides system administrators with a central, easy-to-use console to view critical server and application resources across the enterprise. With AppManager for Nortel CS2x, administrative staff can monitor computer and application resources, check for potential problems, initiate responsive actions, automate routine tasks, and gather performance data for real-time and historical reporting and analysis.

Intended Audience

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

Other Information in the Library

The library provides the following information resources:

Installation Guide for AppManager

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

User Guide for AppManager Control Center

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

Administrator Guide for AppManager

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

Upgrade and Migration Guide for AppManager

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

Management guides

Provide information about installing and monitoring specific applications with AppManager.

Help

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

The AppManager for Nortel CS2x library is available in Adobe Acrobat (PDF) format from the NetIQ Web site: www.netiq.com/support/am/extended/documentation/default.asp?version=AMDocumentation.

Conventions

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

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

About NetIQ Corporation

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

Contacting Sales Support

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

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

Contacting Technical Support

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

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

Contacting Documentation Support

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

Contacting the Online User Community

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

1 Introducing AppManager for Nortel Communication Server 2000/2100

This chapter introduces AppManager for Nortel Communication Server 2000/2100 (Nortel CS2x), providing a brief overview of the module and its architecture.

Nortel Communication Server 2000/2100 is a large-scale, carrier-grade, scalable IP-PBX solutions for consumer and business communication needs, providing traditional voice services and multimedia communications capabilities such as audio and video conferencing, call handling, directory services, instant messaging, and Web collaboration.

NOTE: NetIQ supports Nortel Communication Server 1000 with the AppManager for Nortel CS1000 module.

1.1 Features and Benefits

AppManager helps you gain easy access to Communication Server data, and helps you analyze and manage that data. The AppManager for Nortel CS2x solution minimizes the cost of maintaining Communication Server services and functions, aids in capacity planning, and can prevent downtime. The solution also provides a wide range of diagnostic and management data, which can help prevent outages and keep things running smoothly.

AppManager for Nortel CS2x includes Knowledge Scripts for creating jobs that monitor the health and status of key Communication Server components. These scripts allow you to monitor and manage crucial services at a depth unparalleled by any other solution. You can configure each Knowledge Script to send an alert, collect data for reporting, and perform automated problem management when an event occurs.

The following are just a few of the features and benefits of monitoring Nortel CS2x with AppManager:

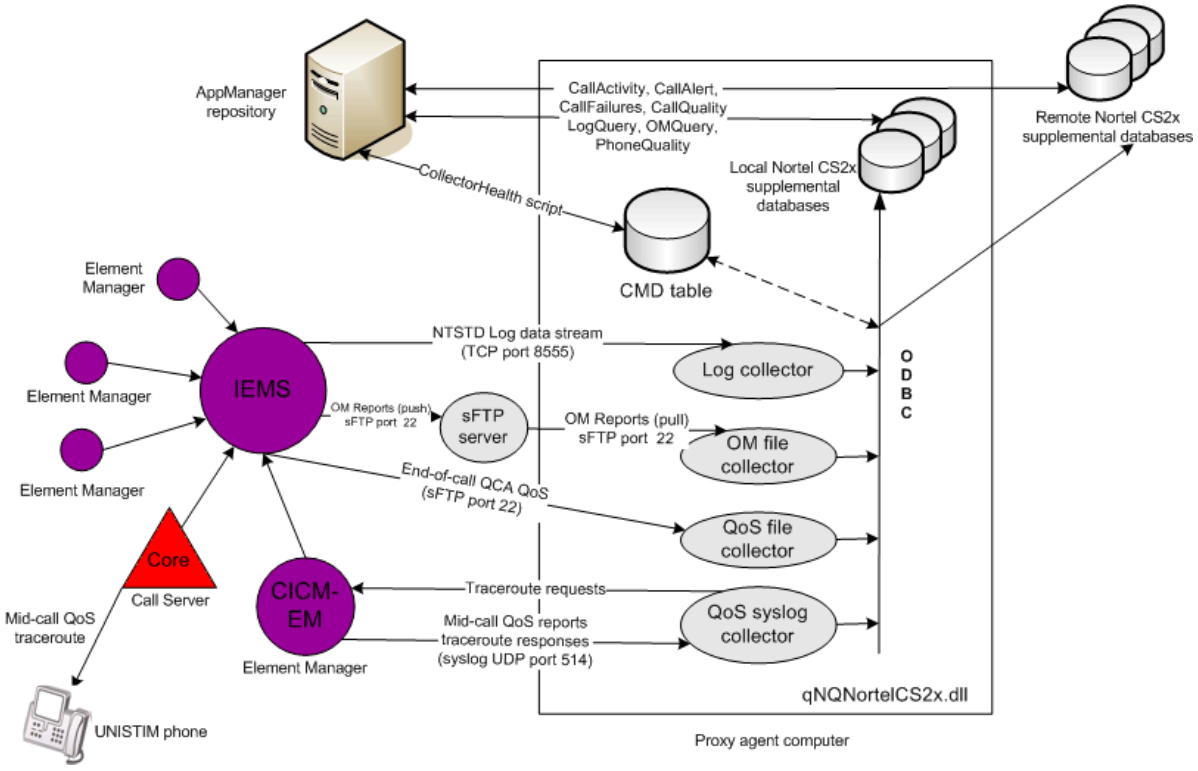
- Monitors the health of system components by monitoring log stream activity and operational measurements:
  - Integrated Element Management System (IEMS) and associated Element Managers
  - Call Server
  - Gateway controllers and gateways
  - Centrex IP Call Managers (CICMs)
  - SIP server
  - Next Generation Session Server (NGSS)
- Monitors availability and activity for collector services
- Monitors completed and active calls

- Monitors real-time, mid-call voice quality statistics from active calls on IP phones: MOS, R-Value, jitter, latency, packet loss
- Monitors end-of-call voice quality statistics from the CICM Element Manager and the CBM: MOS, R-Value, jitter, latency, packet loss
- Monitors LINE (line maintenance) logs for call failures
- Monitors the CICM Element Manager for mid-call alerts (vqalerts)
- Performs queries on specified logs and the OM Report
- Supports Nortel Communication Server version SN11 and SE11. Requires UNISTIM Phase 2 phones for complete call-quality monitoring
- Reduces the time that you spend diagnosing and resolving issues relating to fundamental call-processing functions
- Provides cross-product interaction with NetIQ Vivinet Diagnostics. For more information, see Section 3.16, "Triggering Call and Phone Quality Diagnoses," on page 67.
- Automates system management issues that could affect Nortel CS2x performance

1.2 Understanding the Module Architecture

With AppManager proxy architecture support for monitoring Nortel CS2x, the AppManager agent does not need to be installed on every device that you want to monitor. You can associate a proxy agent computer with only one repository computer. However, you can associate a repository computer with more than one proxy agent computer.

The following diagram illustrates the relationship between Nortel CS2x components, the AppManager repository server, and the proxy agent computer.



You install the AppManager for Nortel CS2x module on the proxy agent computer. Then run the Discovery_NortelCS2x Knowledge Script to configure the collector services and to create the supplemental database on the proxy agent computer or on a remote computer. For more information, see Section 3.14.1, "Understanding the Supplemental Database," on page 63.

- Individual Element Managers and the Core and Billing Manager (CBM) send logs and OM Reports to the IEMS (Integrated Element Management System), which in turn sends the logs to the log collector service and the OM Reports to the OM file collector service over Telnet. The log collector service listens on port 8555. The OM file collector service listens on port 22.

  NOTE: AppManager processes Operational Measurement (OM) files, but the data does not get stored on the OM table of the supplemental database. The OM file collector service does not retrieve or process historical samples, though it will remove historical samples on the sFTP server to manage file space. NortelCS2x Knowledge Scripts that use OM files include: CallActivity, CollectorHealth, and OMQuery.

- The CBM constructs end-of-call QoS Collector Application records from per-call information published by gateway controllers. It then uses sFTP to send these records to the QoS file collector service.
- The CICM Element Manager sends syslogs, mid-call QoS alerts, and traceroute responses to the QoS syslog collector service.
- The CICM Element Manager also sends syslogs containing mid-call QoS records to the UNISTIM phone proxy collector. UNISTIM (Unified Networks IP Stimulus) is a proprietary Nortel VoIP protocol.
- The CollectorHealth Knowledge Script verifies that all collectors are installed and contain data. And, by issuing commands stored in the CMD table in the supplemental database, the CollectorHealth script prompts the collector services to push their data to the appropriate supplemental database using Open Database Connectivity (ODBC).
- The CallActivity, CallAlert, CallFailures, CallQuality, LogQuery, OMQuery, and PhoneDiagnostic and PhoneQuality Knowledge Scripts query the supplemental database for the information you specify.

2 Installing AppManager for Nortel CS2x

This chapter describes system requirements for AppManager for Nortel CS2x and provides installation instructions.

This chapter assumes you have AppManager installed. For more information about installing AppManager or about AppManager system requirements, see the *Installation Guide for AppManager*, which is available on the AppManager Documentation Web site: www.netiq.com/support/am/extended/documentation/default.asp.

2.1 System Requirements

AppManager for Nortel CS2x has the following system requirements:

Software/Hardware	Version
NetIQ AppManager installed on the AppManager repository (QDB) computers, proxy agent computers, and all console computers	At minimum, 7.0 Support for Windows Server 2008 requires hotfix 71704, or the most recent AppManager Windows Agent hotfix. For more information, see the AppManager Suite Hotfixes Web page.
Microsoft operating system on the proxy agent computer	One of the following: ◆ Windows XP Professional SP2 ◆ 32-bit or 64-bit Windows Server 2003 SP2, including R2, Standard or Enterprise Edition ◆ 32-bit or 64-bit Windows Server 2008 SP1 and SP2, Standard or Enterprise Edition ◆ Windows Server 2008 R2
Microsoft SQL Server on the proxy agent computer	One of the following, for support of the Nortel CS2x supplemental database: ◆ 32-bit SQL Server 2005 SP2 ◆ 32-bit SQL Server 2008 Express ◆ 64-bit SQL Server 2008 Enterprise Requires **Microsoft SQL Server 2005 Backward Compatibility Components**, which are part of the **Microsoft SQL Server 2008 Feature Pack**. SQL Server 2008 lacks the SQL-DMO client API required by the Section 3.14, "SetupSupplementalDB," on page 63 Knowledge Script. The Feature Pack contains the necessary API library. For more information, see the Microsoft Download Center Web site.

Software/Hardware	Version
Nortel Communication Server 2100 or 2000	◆ Nortel CS2000: Software version SN10, CVM11, CVM12, CVM13, CVM14, or CVM15 using Phase 2 Unistim phones ◆ Nortel CS2100: Software version SE10, SE11, or SE13 using Phase 2 Unistim phones Note This module can monitor both Nortel CS2000 and CS2100 systems only if all systems are running the same version number. For example, this module supports CS2000 running CVM11 and CS2100 running SE11.
CICM	CICM 11 P9, at minimum CICM 10.1 MR2 P28, at minimum
Microsoft .NET Framework on the proxy agent computer	Version 3 or 3.5, for support of the collector services
Telnet connectivity on the proxy agent computer	To enable log transfers and to enable sFTP connectivity for OM Report transfers
NetIQ Vivinet Diagnostic	Version 2.3 or later, in order to diagnose voice quality problems identified by the CallQuality, PhoneDiagnostic, and PhoneQuality Knowledge Scripts. Install Vivinet Diagnostics on the computer on which the Action_DiagnoseVoIPQuality Knowledge Script runs. Support for Vivinet Diagnostics also requires Microsoft XML Parser version 3 or later, or Microsoft Internet Explorer 5.5, SP2, or later running on the computer on which the Action_DiagnoseVoIPQuality Knowledge Script runs.
AppManager for Microsoft Windows module installed on repository, proxy agent, and console computers	NetIQ recommends version 7.6.170.0, at minimum. For more information, see the AppManager Module Upgrades & Trials Web page.

NOTE: AppManager for Nortel CS2x requires the following corrective content from Avaya product support: CS2x CICM patch sets 10.1MR2 P28 and 11MR2 P9. If you do not apply these patch sets, you might receive events indicating remote throttling at the CS2x or timeouts due to the CICM-EM for the CS2x becoming unresponsive. Apply the most recent patches on both the CICM and the CICM-EM.

For the latest information about supported software versions and the availability of module updates, visit the AppManager Supported Products page at www.netiq.com/support/am/supportedproducts/default.asp. If you encounter problems using this module with a later version of your application, contact NetIQ Technical Support.

2.2 Installing the Module

The setup program automatically identifies and updates all relevant AppManager components on a computer. Therefore, run the setup program only once on any computer. The pre-installation check also runs automatically when you launch the setup program.

You can install the module in one of the following ways:

- Run the module setup program, `AM70-NortelCS2x-7.x.x.0.msi`, which you downloaded from the Web. Save the module setup files on the distribution computer, and then delete the older versions of the module setup files. For more information about the distribution computer, see the *Installation Guide for AppManager*
- Use Control Center to install the module on the remote computer where an agent is installed. For more information, see Section 2.3, "Deploying the Module with Control Center," on page 16.

To install the module:

1. Run the module setup program on all AppManager repository (`QDB`) computers to install the Knowledge Scripts and reports.
   - Run the setup program on the primary repository computer first. Then run the setup program on all other repository computers.
   - For repositories running in active/active and active/passive clusters, run the setup program on the active node. Then, copy the following Registry key to the non-active node.

     `HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\AppManager\4.0`
   - If you are upgrading from version 7.0 to version 7.1 of the module, you must install the module on your repository computers. Version 7.1 will not work if you do not upgrade your repository computers.
   - Install the module on the proxy agent computer. Use one of the following methods:
   - Run the module setup program.
   - Use Control Center to deploy the installation package.
   - If you are upgrading from version 7.0 to version 7.1 of the module, you must install the module on your proxy agent computers. Version 7.1 will not work if you do not upgrade your proxy agent computers.
2. Run the module setup program on all Operator Console and Control Center computers to install the Help and console extensions.
3. Configure the Nortel CS2x switch to work with AppManager. For more information, see Section 2.7, "Configuring Nortel CS2x to Work with AppManager," on page 21.
4. Configure the CICM Element Manager user name and password in AppManager Security Manager. For more information, see Section 2.9.1, "Configuring CICM User Names and Passwords," on page 26.
5. Configure the sFTP server user name and password in AppManager Security Manager. For more information, see Section 2.9.2, "Configuring sFTP User Names and Passwords," on page 26.
6. If you have not discovered Nortel CS2x resources, run the Discovery_NortelCS2x Knowledge Script on all proxy agent computers where you installed the module. You can use Discovery_NortelCS2x to create the remote or local supplemental database. You must create a supplemental database before you can run other NortelCS2x Knowledge Scripts. For more information, see Section 2.6, "Discovering Nortel CS2x Resources," on page 17.

When installation is complete, you can find a record of any problems in the `NortelCS2x_Install.log` file, located in the `\NetIQ\Temp\NetIQ_Debug\<`*ServerName*`>` folder.

2.3 Deploying the Module with Control Center

You can use Control Center to deploy the module on a remote computer where an agent is installed. This topic briefly describes the steps involved in deploying a module and provides instructions for checking in the module installation package. For more information, see the *Control Center User Guide for AppManager*, which is available on the AppManager Documentation Web site: www.netiq.com/support/am/extended/documentation/default.asp.

2.3.1 Deployment Overview

This section describes the tasks required to deploy the module on an agent computer.

To deploy the module on an agent computer:

1. Verify the default deployment credentials.
2. Check in an installation package.
3. Configure an email address to receive notification of a deployment.
4. Create a deployment rule or modify an out-of-the-box deployment rule.
5. Approve the deployment task.
6. View the results.

2.3.2 Checking In the Installation Package

You must check in the installation package, `AM70-NortelCS2x-7.x.x.0.xml`, before you can deploy the module on an agent computer.

To check in a module installation package:

1. Log on to Control Center and navigate to the Administration pane.
2. In the Deployment folder, select **Packages**.
3. On the Tasks pane, click **Check in Packages**.
4. Navigate to the folder where you saved `AM70-NortelCS2x-7.x.x.0.xml` and select the file.
5. Click **Open**. The Deployment Package Check in Status dialog box displays the status of the package check in.

2.4 Silently Installing the Module

You can run the module setup program, `AM70-NortelCS2x-7.x.x.0.msi`, silently (without user intervention) from a command prompt on the local computer.

Run the following command from the directory in which you saved the module setup program. This command installs the module using default settings.

```
msiexec.exe /i "AM70-NortelCS2x-7.x.x.0.msi" /qn
```

where *x.x* is the actual version number of the module setup program.

To create a log file that describes the operations of the module setup program, add the following flag to the command noted above:

```
/L* "AM70-NortelCS2x-7.x.x.0.msi.log"
```

The log file is created in the directory in which you saved the module setup program.

For more information, see "Performing a Silent Installation" in the *Installation Guide for AppManager*.

2.5 Verifying Your Installed Module

To verify installation on many computers, run the ReportAM_CompVersion Knowledge Script. Ensure you discover a report-enabled agent before running this script. For more information, see the Help for the script.

To verify installation on one or only a few computers, use the Operator Console.

To verify your installed module with the Operator Console:

1. In the TreeView pane, select the computer for which you want to verify your installed module.
2. From the TreeView menu, select **Properties**. On the System tab, the System information pane displays the version numbers for all modules installed on the computer.
3. Verify that the version number from the *AppManager for Nortel Communication Server 2000/2100 Readme* matches the version number shown in the System information pane.

2.6 Discovering Nortel CS2x Resources

Use the Discovery_NortelCS2x Knowledge Script to create the Nortel CS2x supplemental database and to configure the services that collect data from Nortel CS2x components:

- Integrated Element Management System (IEMS)
- Element Managers
- Centrex IP Call Managers (CICM)

For more information, see Section 1.2, "Understanding the Module Architecture," on page 10.

Before discovering resources, perform the following tasks:

- Configure Nortel CS2x to work with AppManager. For more information, see Section 2.7, "Configuring Nortel CS2x to Work with AppManager," on page 21.
- Configure AppManager Security Manager with the user names and passwords that permit access to CS2x components. For more information, see Section 2.9, "Configuring User Names and Passwords in Security Manager," on page 25.
- For a remote supplemental database, prepare the remote computer for creation of the supplemental database. For more information, see Section 2.10, "Configuring the Remote Supplemental Database Computer," on page 27.

Set the parameters on the Values tab as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	

Parameter	How to Set It
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Discovery_NortelCS2x Knowledge Script job fails. The default is 5.
Raise event if discovery succeeds?	Select **Yes** to raise an event if the supplemental database is created and the collector services are configured. The default is Yes.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the supplemental database is created and the collector services are configured. The default is 25.
Raise event if discovery fails?	Select **Yes** to raise an event if the supplemental database is not created or the collector services are not configured. The default is Yes.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the supplemental database is not created or the collector services are not configured. The default is 5.
Unique identifier of the switch to discover	Provide the unique, common name of the CS2x office you want to discover. The common name is displayed in the logs created by the CS2x. As a best practice, the common name you enter here should match the office name in one of the following locations: ◆ `LOG_OFFICE_ID` in the core table `OFCVAR` ◆ `OFFICE_CLLI_NAME` ◆ Office log name in the IEMS **NOTE**: Do not leave this field blank.
IP address of the IEMS	Provide the IP address of the IEMS you want to discover.
Supplemental Database Creation	
Set up supplemental database?	Select **Yes** to create the Nortel CS2x supplemental database, including the tables and stored procedures needed to store log files, OM Reports, call details, and QoS information. When the database is populated, you can monitor the data using the CallActivity, CallQuality, LogQuery, OMQuery, PhoneDiagnostic, and PhoneQuality Knowledge Scripts. You can also create the supplemental database after you run the Discovery script. For more information, see SetupSupplementalDB.
Database Record Retention	
Number of days to keep supplemental database records	Specify the number of days you want to keep records in the Nortel CS2x supplemental database. Data older than that is discarded. The default is 14 days.
SQL Server Information	

Parameter	How to Set It
SQL Server computer name	Specify the DNS name or IP address of the SQL Server computer on which you want to create the remote Nortel CS2x supplemental database. Leave this parameter blank to create the supplemental database on the proxy agent computer. For either a remote or local supplemental database, configure the SQL Server user name and password in AppManager Security Manager. For more information, see Section 2.9.3, “Configuring SQL Server User Names and Passwords,” on page 27.
SQL Server instance name	Specify the name of the SQL Server instance on the computer on which you want to create the Nortel CS2x supplemental database. Leave this parameter blank to accept the default instance name.
Raise event if database setup succeeds?	Select **Yes** to raise an event if creation of the Nortel CS2x supplemental database is successful. The default is unselected.
Event severity when database setup succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the success of the creation of the Nortel CS2x supplemental database. The default is 25.
Configuration Data Retrieval	
Retrieve configuration data from IEMS?	Select **Yes** to retrieve station configuration information from individual CICM Element Managers and store it in the Nortel CS2x supplemental database, where it can be monitored by the PhoneInventory Knowledge Script. You can also retrieve station configuration information after you run the Discovery script. For more information, see RetrieveConfigData.
Log Collector Service	
Configure log collector service?	Select **Yes** to create and start the log collector service on the proxy agent computer. The default is Yes. Element Managers push logs to the log collector service over Telnet. Associated Knowledge Scripts are CallFailures, LogQuery, and OMQuery.
Server address to receive log messages from	Specify the IP address of the Element Manager that will send logs. Leave this field blank if the address is that of the IEMS.
Port number to receive log messages from	Specify the port number on the proxy agent computer that will listen for logs. The default port number is 8555.

Parameter	How to Set It
Timestamp offset for time zone differences on log messages	If your CS2x office and proxy agent computer are in different time zones, use this parameter to adjust the timestamps on the logs sent by the CS2x. For example, if the time zone of your proxy agent computer is three hours *ahead* of the CS2x that is sending logs, the difference in minutes is 180. So specify `180` in this parameter. If the time zone of your proxy agent computer is three hours *behind* that of your CS2x, specify `-180` in this parameter. **Note about Daylight Savings Time** You may need to manually adjust the timestamp offset at the Spring and Fall time change for Daylight Savings Time (DST). If your query Knowledge Script jobs (CallActivity, CallFailures, CallQuality, LogQuery, and OMQuery) return no data, but data has been collected and stored in the supplemental database, verify the timestamps in the data. If the timestamps have been affected by DST, rerun the Discovery script using a new timestamp offset value.
OM File Collector Service	
Configure OM file collector service?	Select **Yes** to create and start the OM file collector service on the proxy agent computer. The default is Yes. Element Managers send OM Reports to the IEMS, which in turn sends the OM Reports to the OM file collector service over sFTP. The associated Knowledge Script is CallActivity.
Server address to receive sFTP OM Reports from	Specify the IP address of the Element Manager that will send OM Reports over sFTP. Leave this field blank if the address is that of the IEMS.
Port number to receive sFTP OM Reports from	Specify the port number on the proxy agent computer that will listen over sFTP for OM Reports. The default port number is 22.
Directory location at sFTP server to retrieve sFTP OM Reports from	Specify the name of the directory on the sFTP server from which to retrieve the OM Reports. **NOTE**: Do not leave this field blank.
Timestamp offset for time zone differences on sFTP OM Reports	If your CS2x office and proxy agent computer are in different time zones, use this parameter to adjust the timestamps on the OM Reports sent by the CS2x. For example, if the time zone of your proxy agent computer is three hours *ahead* of the CS2x that is sending OM Reports, the difference in minutes is 180. So specify `180` in this parameter. If the time zone of your proxy agent computer is three hours *behind* that of your CS2x, specify `-180` in this parameter. **Note about Daylight Savings Time** You may need to manually adjust the timestamp offset at the Spring and Fall time change for Daylight Savings Time (DST). If your query Knowledge Script jobs (CallActivity, CallFailures, CallQuality, LogQuery, and OMQuery) return no data, but data has been collected and stored in the supplemental database, verify the timestamps in the data. If the timestamps have been affected by DST, rerun the Discovery script using a new timestamp offset value.
QoS Syslog Collector Service	

Parameter	How to Set It
Configure QoS syslog collector service?	Select **Yes** to create and start the QoS syslog collector service on the proxy agent computer. The default is Yes. The QoS syslog collector service receives end-of-call QoS syslogs from CICM Element Managers. The associated Knowledge Script is CallQuality.
Server address to receive QoS syslog reports from	Specify the IP address of the Element Manager that will send QoS syslog reports. Leave this field blank if the address is that of the IEMS.
Port number to receive QoS syslog reports on	Specify the port number on the proxy agent computer that will listen for syslogs reports. The default port number is 514.
QoS File Collector Service	
Configure QoS file collector service?	Select **Yes** to create and start the QoS file collector service on the proxy agent computer. The default is Yes. Element Managers send QoS reports to the IEMS, which in turn sends the QoS reports to the QoS file collector service over sFTP. The associated Knowledge Script is CallQuality.
Server address to receive QoS files from	Specify the IP address of the CBM that will send QoS files over sFTP. Leave this field blank if the address is that of the IEMS.
Port number to receive QoS files from	Specify the port number on the proxy agent computer that will listen over sFTP for QoS files. The default port number is 22.
Directory location at sFTP server to receive active QCA file	Specify the name of the directory on the sFTP server from which to retrieve the QoS Collector Application file containing the QoS data. **NOTE**: Do not leave this field blank.

2.7 Configuring Nortel CS2x to Work with AppManager

Complete all of the following configuration tasks to allow the Nortel CS2x switch to work with AppManager and the AppManager for Nortel CS2x module.

Requirement	Description
Read/write login account (user name and password) to sFTP on the IEMS	1. Contact your Nortel CS2x administrator to create this account. For more information, see Nortel document NN10336-611: *Carrier VoIP: IEMS Administration and Security*. Configure the read/write user name and password in AppManager Security Manager. For more information, see Section 2.9.2, "Configuring sFTP User Names and Passwords," on page 26.

Requirement	Description
Set up log destination	2. On the IEMS (Integrated Element Management System), configure the proxy agent computer IP address as a log destination. For more information, see Nortel document NN10334-911: *Integrated EMS Fault Management*. At the IEMS, navigate to the Runtime Administration window. In the tree pane, expand the **Categories** folder, expand the **OSS Config** folder, and then select the **NTSTD** node. In the **Manager Host** field, provide the proxy agent computer IP address. In the **Office Identifier** field, provide the office identifier of the CS2x switch. As a best practice, use the same identifier you use in the *Unique identifier of the switch to discover* parameter in the Discovery_NortelCS2x Knowledge Script. Click **Add** and then click **Apply**. **Notes** ◆ If the proxy agent computer is outside the firewall, configure the firewall address rather than the proxy agent computer address. ◆ Ensure TCP port 8555 (the NTSTD port) is open on the firewall between the proxy agent computer and the IEMS.
Enable QoS reporting	3. Set up QoS collection at the GWC (gateway controller) Element Manager. Access the CS2000 Management Tools application. Expand the **Device Types** folder and select **Gateway Controller**. In the Gateway Controllers panel, select the GWC you want to configure. On the QoS Collectors tab, select **Enable QoS Collection**. On the File menu, select **Save**. For more information, see Nortel document NN10240-511: *Carrier VoIP: Nortel CICM Configuration*.

Requirement	Description
Set up OM Report collection	4. Set up an FTP dropbox server that supports both FTP and sFTP. ◆ Perform a manual sFTP to the dropbox server to obtain the certificate. Use the following command: `sftp xxx.xxx.xxx.xxx userid` where `xxx.xxx.xxx.xxx` is the IP address of the dropbox server and `userid` is the userid for the dropbox server. ◆ The manual sFTP process stores the `known_hosts` file in the `/.ssh` directory ◆ Copy the `known_hosts` file to `/cbmdata/users/maint/.ssh`. ◆ If `known_hosts` already exists in the `/cbmdata/users/maint/.ssh` directory, then edit it to add the certificate for the dropbox server. On the CBM (Core and Billing Manager), configure the sFTP server as a file transfer destination. ◆ Log in to the active CBM. ◆ From the OM Delivery Main Menu, select option 4: **File Transfer Destination**. ◆ For **File Transfer Destination name**, type `netiq`. ◆ For **Destination IP Address**, type the IP address of the sFTP server. ◆ For **Type of file transfer**, type `secure`. ◆ For **Type of Authentication**, type `password`. ◆ For **Destination Login**, type the login for the sFTP server. ◆ For **Destination Password**, type the password for the sFTP server. ◆ Press `[Enter]` and type `y` at the **Add File Transfer Destination (Y/N)?** prompt. On the CBM, add the following OM Report groups to a report element: SITE, PM, LMD, TRK, CP, SITE2, XPMOVLD. ◆ Log in to the active CBM. ◆ From the OM Delivery Main Menu, select option 1: **Report Element**, and then select option 2: **Add Report Element**. ◆ For **Report element name**, type `netiq`. ◆ For **Reporting interval**, type 2. ◆ For **OM group name**, type `SITE`. ◆ For **Register or All**, type `All`. ◆ For **Add OM group (Y/N)?**, type `y`. ◆ Press `[Enter]` and type `y` at the **Add report element (Y/N)?** prompt. ◆ Repeat for each required OM report group. For more information, see Nortel document NN10148-711: *Carrier VoIP: Nortel CS2000 Core Manager Performance Management*.

Requirement	Description
Enable syslog delivery	5. Configure the proxy agent computer as the destination for the CICM syslogs. Access the Centrex IP Client Manager and navigate to the Global Settings Modification page. On the Global tab, provide the proxy agent computer IP address in the **Extended QoS server Ip Address** field. In the **Extended QoS server port** field, provide the port number on the proxy agent computer that will listen for syslogs. Enter the same port number you use in the *Port number to receive QoS syslog messages on* parameter in the Discovery_NortelCS2x Knowledge Script. In the Discovery script, port 514 is the default port number. If port 514 is in use, select another port number and ensure you indicate the same port number in the Discovery script.
Enable delivery of voice quality alerts	6. Create a Voice Quality Monitoring (vqmon) profile on the CICM Element Manager. The vqmon profile allows AppManager to receive the alerts monitored by the CallAlert Knowledge Script. Access the Centrex IP Client Manager and navigate to the vqmon Profiles page. In the **Profile name** field, type `netiq`. Accept the **Default Value** for all other fields. Click **Save your changes to this profile**.

2.8 Summary of Port and IP Address Requirements

The following table summarizes the source and destination ports identified in the drawing in Section 1.2, "Understanding the Module Architecture," on page 10 and discussed in Section 2.7, "Configuring Nortel CS2x to Work with AppManager," on page 21

Component	Packet Type	Source IP	Source Port	Destination IP	Destination Port
Log collector	TCP Two-way filter	IP address for the computer that hosts the log collector.	Dynamic	IEMS IP address provided in the parameters for Discovery_NortelCS2x	8555, by default. You can change this port number when you run the Discovery script.
OM file collector	TCP Two-way filter	IP address for the CBM. Appears in the IEMS inventory data as `<addr>,GWC Mgr`. You will have only one of these addresses.	Dynamic	IP address of the OM sFTP dropbox server Can be installed on the proxy agent computer or on a remote computer	sFTP port 22, by default

Component	Packet Type	Source IP	Source Port	Destination IP	Destination Port
OM file collector	TCP Two-way filter	IP address for the computer that hosts the OM file collector If OM file collector and OM dropbox are located on the same computer, both sides of this filter can be set to `127.0.0.1` or a loopback address. If the collector and dropbox are not co-located, use the actual network IP address.	Dynamic	IP address of the OM sFTP dropbox server Can be installed on the proxy agent computer or on a remote computer	sFTP port 22, by default
Inventory data retrieval	TCP Two-way filter	IP address of the proxy agent computer	Dynamic	IEMS IP address provided in the parameters for Discovery_NortelCS2x	sFTP port 22, by default
Station data retrieval	TCP Two-way filter	IP address of the proxy agent computer	Dynamic	CICM Element Manager floating IP address Will appear in the TreeView after you run Discovery_NortelCS2x	HTTPs port 443, by default
QoS file collector	TCP Two-way filter	IP address of the computer that hosts the Qos file collector	Dynamic	IEMS IP address provided in the parameters for Discovery_NortelCS2x	sFTP port 22, by default
QoS syslog collector	UDP	CICM Element Manager floating IP address Appears in the IEMS inventoryData file as `<addr>CICM` You may have more than one of these addresses. Enter each as a source address.	Dynamic	IP address of the computer that hosts the QoS syslog collector	UDP port 514, by default. You can change this port number when you run the Discovery script.

.

2.9 Configuring User Names and Passwords in Security Manager

Several AppManager for Nortel CS2x Knowledge Scripts and collector services require access to various components of the Nortel CS2x environment. Configure AppManager Security Manager with the user names and passwords that permit access to the components.

2.9.1 Configuring CICM User Names and Passwords

The RetrieveConfigData Knowledge Script retrieves station configuration information from individual CICM Element Managers. Before running the RetrieveConfigData Knowledge Script, configure AppManager Security Manager with the user name and password of the CICM Element Manager. This information allows AppManager to access the configuration information in the Element Managers.

On the Custom tab in Security Manager, complete the following fields:

Field	Description
Label	`NortelCS2x_CICM-EM`
Sub-label	The name of the switch associated with the Element Manager. This is the same information you provide in the *Unique identifier of the switch to discover* parameter in the Discovery_NortelCS2x Knowledge Script. Or, type `default` if the user name and password apply to all switches.
Value 1	The Element Manager user name.
Value 2	The Element Manager password.
Extended application support	Required. Encrypts the user name and password in Security Manager.

2.9.2 Configuring sFTP User Names and Passwords

The OM file collector service and QoS file collector service receive data over secure FTP (sFTP). Before you run the Discovery_NortelCS2x Knowledge Script, configure AppManager Security Manager with the user name and password of the associated sFTP server.

On the Custom tab in Security Manager, complete the following fields:

Field	Description
Label	◆ For the OM file collector service: `NortelCS2x_OMFileCollector`. ◆ For the QoS file collector service: `NortelCS2x_QoSFileCollector`.
Sub-label	The name of the switch associated with the sFTP server. This is the same information you provide in the *Unique identifier of the switch to discover* parameter in the Discovery_NortelCS2x Knowledge Script. Or, type `default` if the user name and password apply to all switches.
Value 1	The sFTP user name.
Value 2	The sFTP password.
Extended application support	Required. Encrypts the user name and password in Security Manager.

2.9.3 Configuring SQL Server User Names and Passwords

The Discovery_NortelCS2x and SetupSupplementalDB Knowledge Scripts require access to the SQL Server database on the remote computer on which you want to install the Nortel CS2x supplemental database. Before you run the Discovery or SetupSupplementalDB scripts, configure AppManager Security Manager with the user name and password of the remote SQL Server computer.

On the Custom tab in Security Manager, complete the following fields:

Field	Description
Label	`NortelCS2x_Database`
Sub-label	The unique, common name of the CS2x office that contains the remote computer on which you want to create the Nortel CS2x supplemental database. Use the same name you entered in the *Unique identifier of the switch to discover* parameter in the Discovery_NortelCS2x Knowledge Script. `Default` is an acceptable value for this parameter.
Value 1	The SQL Server user name for the remote computer on which you want to create the Nortel CS2x supplemental database.
Value 2	The SQL Server password associated with the user name you supplied in the Value 1 field.
Extended application support	Required. Encrypts the user name and password in Security Manager.

2.10 Configuring the Remote Supplemental Database Computer

Take the following steps to prepare a SQL Server computer for creation of the remote supplemental database.

To set up the remote SQL Server computer:

1. Use SQL Server Configuration Manager to disable dynamic ports.
2. Use SQL Server Configuration Manager to enable **TCP/IP** on the instance object where you want to create the remote supplemental database.
3. Use Microsoft SQL Server Management Studio to enable **SQL Server and Windows Authentication mode** on the instance object where you want to create the remote supplemental database.
4. Create a new SQL Server user name and password. Assign the new user both `sysadmin` and `processadmin` privileges.
5. In AppManager Security Manager, configure the new user name and password. For more information, see Section 2.9.3, "Configuring SQL Server User Names and Passwords," on page 27.

3 NortelCS2x Knowledge Scripts

AppManager for Nortel CS2x provides Knowledge Scripts for monitoring Nortel Communication Server 2000 and 2100 resources.

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

Knowledge Script	What It Does
AddPhone	Adds Nortel IP phones to the AppManager console for monitoring by the PhoneQuality and PhoneDiagnostic Knowledge Scripts.
CallActivity	Monitors completed and peak active calls.
CallAlert	Monitors for mid-call alerts raised when voice quality thresholds are exceeded. Can launch Vivinet Diagnostics to diagnose the problem if alerts are received.
CallFailures	Monitors the following line maintenance logs for call failure data: 101, 102, 104, 105, 115, 138, and 160. You can monitor all or some of these logs.
CallQuality	Monitors end-of-call voice quality statistics: jitter, latency, packet loss, MOS (Mean Opinion Score), and R-Value.
CollectorHealth	Starts the collector services and monitors their activity and availability.
LogQuery	Monitors the number of logs in user-specified reports.
OMQuery	Monitors the contents of specified fields in OM Reports.
PhoneDiagnostic	Launches Vivinet Diagnostics on-demand to diagnose call quality between two specified phones.
PhoneInventory	Creates an inventory of the phones configured for an Element Manager.
PhoneQuality	Monitors mid-call voice quality statistics: jitter, latency, packet loss, MOS (Mean Opinion Score), and R-Value.
RemovePhone	Removes a Nortel IP phone from the AppManager console.
RetrieveConfigData	Retrieves station configuration information from individual CICM Element Managers and stores it in the Nortel CS2x supplemental database for monitoring by the PhoneInventory script.
SetupSupplementalDB	Creates a Nortel CS2x supplemental database in which to store log files, OM Reports, call details, QoS information, and station configuration information.
Recommended Knowledge Script Group	Performs essential monitoring of your Nortel CS2x environment.

3.1 AddPhone

Use this Knowledge Script to add Nortel IP phones (stations) to the AppManager console. This script raises an event if specified phones are added successfully or cannot be added.

You must add a phone before you can monitor it with the PhoneQuality or PhoneDiagnostic Knowledge Script.

Use the RemovePhone Knowledge Script to remove a phone.

3.1.1 Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the supplemental database.
- Run RetrieveConfigData to populate the supplemental database. The IP addresses and Directory Numbers (DNs) of the phones you want to add must have an entry in the supplemental database, or the AddPhone job will fail.

3.1.2 Resource Object

NortelCS2x Station Folder

3.1.3 Default Schedule

By default, this script runs once.

3.1.4 Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the AddPhone job fails. The default is 5.
Configuration Settings	
Directory Numbers of phones to add	Provide the DNs of the phones you want to add. You can provide one DN or a list of DNs. If you enter a list, separate the entries with a comma. For example: `74567,74569,74571`. **NOTE**: If you have more DNs than is convenient to enter in this field, you can list the DNs in a separate file and then use the following parameter to access that file.

Description	How To Set It

Full path to file with list of Directory Numbers of phones to add	Provide the full path to a file that contains a list of the Directory Numbers you want to add. Each address in the file should be on a separate line. For example:
	
	`74567`
	`74569`
	`74571`
	
	Because the file must be accessible from the agent computer, the path must be a local directory on the agent computer or a UNC path.
	
	Important If you provide a UNC path, then the `netiqmc` service must have access to the path.

Allow non-existent phones to be added?	Select **Yes** to add non-existent phones. A phone is non-existent if its number is not in the station table. You can add a non-existent phone if you are sure the phone is valid. For example, you may have just plugged in the phone and do not want to wait for a station table update to test it. The default is unselected.
Default Configuration Settings for Non-Existent Phones	
Default node ID	Provide the alpha-numeric CICM node identifier for the phone you want to add, such as `cicm-005`.
Default terminal ID	Provide the terminal identifier of the phone you want to add, which is usually a MAC address. For example, `31-38-00-0A-E4-01-DA-82`.
Event Notification	
Raise event if all phones are added successfully?	Select **Yes** to raise an event if each phone is successfully added to the AppManager console. The default is Yes.
Event severity when all phones are added successfully	Set the event severity level, from 1 to 40, to reflect the importance of an event in which each phone is added successfully. The default is 25.
Raise event if too many phones to add?	Select **Yes** to raise an event if, by running this job, you will have added more than 500 phones per office configured in the AppManager console. The default is Yes.
Event severity when too many phones to add	Set the event severity level, from 1 to 40, to reflect the importance of an event in which you have attempted to add more than 500 phones to an office configured in the AppManager console. The default is 15.

3.2 CallActivity

Use this Knowledge Script to monitor call activity on a selected CS2x. This script raises an event if the number of completed calls and the maximum number of concurrent active calls exceed the thresholds you set. In addition, this script generates data streams for completed and active calls.

This script uses the data collected by the OM file collector service and stored in the supplemental database.

3.2.1 Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the supplemental database.
- Run CollectorHealth to start the OM file collector service.

3.2.2 Resource Object

NortelCS2x

3.2.3 Default Schedule

By default, this script runs every five minutes.

You may notice a large difference between the timestamp of the data point (generated every five minutes on the default schedule) and the timestamp of the OM Report that provides the data for this script. The OM Report interval varies, but is typically every five, 30, or 60 minutes. The timestamp of the OM Report represents the beginning of the interval. For example, if the OM Report for the calls made from 9:00 to 9:30 is sent at 9:30, the timestamp is 9:00. The data point will have a timestamp of a few minutes past 9:30, depending on when the five-minute default interval ends.

3.2.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CallActivity job fails. The default is 5.
Raise event if data collector reports an error?	Select **Yes** to raise an event if the OM file collector service reports an error. The default is Yes. An error affects the entire data-collection connection and all data associated with that connection.
Event severity when data collector reports an error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the OM file collector service reports an error. The default is 5.
Raise event if data collector reports a transaction error?	Select **Yes** to raise an event if the OM file collector service reports a transaction error. The default is Yes.
Event severity when data collector reports a transaction error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the OM file collector service reports a transaction error. The default is 10.
Raise event if data collector reports a warning?	Select **Yes** to raise an event if the OM file collector service reports a warning. The default is Yes.
Event severity when data collector reports a warning	Set the severity level, from 1 to 40, to indicate the importance of an event in which the OM file collector service reports a warning. The default is 15.
Troubleshooting	
Select time range	Select a **Specific** or **Sliding** date/time range for which the query should search for data. The default time range is fixed at 24 hours. **NOTE**: This parameter is valid only when you select **Run once** on the Schedule tab.
Location Filter	

Parameter	How to Set It
Include or exclude specific locations	Select the IEMS systems for which you want to monitor call activity. ◆ Select **Include only** to monitor call activity from the system specified in the *Location* parameter. ◆ Select **Exclude** to monitor call activity for all systems except the system specified in the *Location* parameter. The default is Exclude.
Location	Provide the name of the IEMS system that you want to include or exclude from monitoring.
Monitor Total Completed Calls	
Event Notification	
Raise event if total number of completed calls exceeds threshold?	Select **Yes** to raise an event if the number of completed calls exceeds the threshold you set. The default is Yes.
Threshold - Maximum total number of completed calls	Specify the maximum number of calls that can be completed before an event is raised. The default is 100 active call.
Event severity when total number of completed calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of completed calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for total number of completed calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of calls completed during the monitoring period. The default is Yes.
Monitor Concurrent Active Calls	
Event Notification	
Raise event if maximum number of concurrent active calls exceeds threshold?	Select **Yes** to raise an event if the maximum number of concurrent active calls exceeds the threshold you set. The default is Yes. *Concurrent active calls* are calls that are in progress at the same time during a monitoring interval. Use this set of parameters to monitor the maximum number of concurrent calls that are in progress at any point in time. For example, during a five-minute interval, ten calls are active at one moment, seven calls are active at another, and three active at yet another moment. Therefore, for this interval, the maximum number of concurrent active calls is ten.
Threshold - Maximum number of concurrent active calls	Specify the maximum number of concurrent calls that can be active at any point in time before an event is raised. The default is 100 active calls.
Event severity when number of concurrent active calls exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of concurrent active calls exceeds the threshold. The default is 15.
Data Collection	
Collect data for maximum number of concurrent active calls?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the maximum number of concurrent calls that were active during the monitoring period. The default is Yes.

3.3 CallAlert

Use this Knowledge Script to monitor mid-call alerts (vqalerts) generated when voice quality metrics exceed or fall below a threshold you set on the CICM Element Manager. This script raises an event if vqalerts are generated. You can filter results by vqalert and by phone, and you can launch NetIQ Vivinet Diagnostics to diagnose the problem if vqalerts are generated. For more information, see Section 3.16, "Triggering Call and Phone Quality Diagnoses," on page 67.

3.3.1 Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the supplemental database.
- Run CollectorHealth to start the QoS syslog collector service.

3.3.2 Resource Object

NortelCS2x

3.3.3 Default Schedule

By default, this script runs on an asynchronous schedule.

3.3.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CallAlert job fails. The default is 5.
Raise event if data collector reports an error?	Select **Yes** to raise an event if the QoS syslog collector service reports an error. The default is Yes. An error affects the entire data-collection connection and all data associated with that connection.
Event severity when data collector reports an error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the QoS syslog collector service reports an error. The default is 10.
Raise event if data collector reports a warning?	Select **Yes** to raise an event if the QoS syslog collector service reports a warning. The default is Yes.
Event severity when data collector reports a warning	Set the severity level, from 1 to 40, to indicate the importance of an event in which the QoS syslog collector service reports a warning. The default is 15.
Monitor Settings	
Perform traceroute and launch Vivinet Diagnostics when voice quality alert is received?	Select **Yes** to send a traceroute request to the CICM Element Manager and to launch Vivinet Diagnostics to diagnose the problem if vqalerts are received. The default is Yes.

Parameter	How to Set It
Length of time to wait for traceroute responses	Specify the maximum length of time that the CallAlert job should wait for a response to traceroute requests to the CICM Element Manager. The CallAlert job will fail if the response time is longer than you specify. The default is 120 seconds.
Raise event if voice quality alert is received?	Select **Yes** to raise an event if vqalerts are generated when voice quality metrics exceed the threshold you set on the CICM Element Manager. The default is Yes.
Event severity when voice quality alert is received	Set the severity level, from 1 to 40, to indicate the importance of an event in which vqalerts are generated when voice quality metrics exceed the threshold you set on the CICM Element Manager. The default is 15.
Include or exclude specific voice quality alerts	Indicate how to monitor the vqalerts you select in the *Alert filter* parameters. The default is Exclude. ◆ Select **Include** to monitor only the selected vqalerts. ◆ Select **Exclude** to monitor all vqalerts *except* those that you select.
Alert Filter	
Minor alert: packet loss threshold crossed?	Select **Yes** to monitor the number of minor alerts generated when packet loss (LRA-Loss Rate Average) exceeds the threshold you set in Element Manager. The default is unselected.
Minor alert: one-way latency threshold crossed?	Select **Yes** to monitor the number of minor alerts generated when one-way latency (OWDA-One Way Delay Average) exceeds the threshold you set in Element Manager. The default is unselected.
Minor alert: round-trip latency threshold crossed?	Select **Yes** to monitor the number of minor alerts generated when round-trip latency (RTA-Round Trip Average) exceeds the threshold you set in Element Manager. The default is unselected.
Minor alert: jitter threshold crossed?	Select **Yes** to monitor the number of minor alerts generated when jitter (JA-Jitter Average) exceeds the threshold you set in Element Manager. The default is unselected.
Minor alert: R-factor threshold crossed?	Select **Yes** to monitor the number of minor alerts generated when the R-factor value (LRF-Listening R Factor) falls below the threshold you set in Element Manager. The default is unselected.
Major alert: packet loss threshold crossed?	Select **Yes** to monitor the number of major alerts generated when packet loss exceeds the threshold you set in Element Manager. The default is unselected.
Major alert: one-way latency threshold crossed?	Select **Yes** to monitor the number of major alerts generated when one-way latency exceeds the threshold you set in Element Manager. The default is unselected.
Major alert: round-trip latency threshold crossed?	Select **Yes** to monitor the number of major alerts generated when round-trip latency exceeds the threshold you set in Element Manager. The default is unselected.
Major alert: jitter threshold crossed?	Select **Yes** to monitor the number of major alerts generated when jitter exceeds the threshold you set in Element Manager. The default is unselected.
Major alert: R-factor threshold crossed?	Select **Yes** to monitor the number of major alerts generated when the R-factor value falls below the threshold you set in Element Manager. The default is unselected.

Parameter	How to Set It
Include or exclude specific phones	You can further filter your results by monitoring vqalerts only for phones you specify in the *Phone filter* parameters. The default is Exclude. ◆ Select **Include** to monitor vqalerts only for the selected phones. ◆ Select **Exclude** to monitor vqalerts for all phones *except* those that you select.
Phone Filter	
Enterprise Network Association Name	Provide the network name associated with the phones for which you want to monitor vqalerts. This network name identifies a grouping of phones behind a firewall.
Phone Enterprise IP address	For the phones associated with the *Enterprise Network Association Name*, provide the IP address used as the bearer path before it gets to the firewall. Separate multiple addresses with a comma. An asterisk (*) is an acceptable wildcard.

3.4 CallFailures

Use this Knowledge Script to monitor LINE (line maintenance) logs. The line maintenance subsystem generates LINE logs for specific occurrences, as detailed below. This script monitors LINE logs retrieved through telnet from the IEMS and collected by the log collector service.

You can monitor all or some of the following LINE logs, which are related to call failures:

- **LINE101**, generated when the system or the user runs a diagnostic test that fails.
- **LINE102**, generated when the system changes the line state from call processing busy (CPB) to lockout (LO). LINE 102 often indicates a facility problem.
- **LINE104**, generated when a problem occurs during call processing or when bearer path integrity issues are detected.
- **LINE105**, indicates permanent signal, usually a phone left offhook, but may be a line or equipment problem
- **LINE115**, generated at the termination of a call that is connected to the DMS switch but originated from another line.
- **LINE138**, generated when a call routes to a treatment, such as automated voice response.
- **LINE160**, generated when the called party does not answer within the ringing timeout period.

The purpose of this script is twofold:

- **Monitoring**. In monitoring mode, this script checks the database tables at each specified interval for new records that match your query. In the first iteration of the job, this script finds the last record in a table and checks back one interval from there. In subsequent iterations, this script checks for new records that match the query in each interval.
- **Troubleshooting**. In troubleshooting mode, this script runs once and checks the database tables for calls whose disconnect time is within the range you select in the *Select call disconnect time range* parameter. Select **Run once** on the Schedule tab to run this script in troubleshooting mode. The managed object does not collect call quality statistics unless this script is running, which could pose a problem should you want, for example, to troubleshoot a call that occurred five minutes ago. To perform troubleshooting as needed, also run CollectorHealth to start the collector services, which populate the Nortel CS2x supplemental database with data you can use for troubleshooting.

3.4.1 Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the supplemental database.
- Run CollectorHealth to start the log collector service.

3.4.2 Resource Object

NortelCS2x

3.4.3 Default Schedule

By default, this script runs every five minutes.

3.4.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CallFailures job fails. The default is 5.
Raise event if data collector reports an error?	Select **Yes** to raise an event if the log collector service reports an error. The default is Yes. An error affects the entire data-collection connection and all data associated with that connection.
Event severity when data collector reports an error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the log collector service reports an error. The default is 5.
Raise event if data collector reports a transaction error?	Select **Yes** to raise an event if the log collector service reports a transaction error. The default is Yes. A transaction error affects a single record encountered during the data-collection connection. If there are many transaction errors for the same record, only the most recent transaction error is posted for each iteration of the connection.
Event severity when data collector reports a transaction error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the log collector service reports a transaction error. The default is 10.
Raise event if data collector reports a warning?	Select **Yes** to raise an event if the log collector service reports a warning. The default is Yes.
Event severity when data collector reports a warning	Set the severity level, from 1 to 40, to indicate the importance of an event in which the log collector service reports a warning. The default is 15.

Parameter	How to Set It
Include log details?	Select **Yes** to include log details in the events raised by this script. Leave this parameter unselected to suppress log details. When you select Yes, an event includes the following columns: ◆ Severity ◆ Report Name ◆ Report Number ◆ Report Time ◆ SequenceSS (a unique identifier for a log) ◆ SequenceDD (a unique identifier for a log) ◆ Event Type ◆ Event ID ◆ Report Details
Maximum table size	If you selected Yes for *Include log details?*, specify the maximum number of rows of log detail that you want to return in events raised by this script. The default is 25 rows.
Troubleshooting	
Select call disconnect time range	Select a **Specific** or **Sliding** date/time range for which the query should search for data. The default time range is fixed at 24 hours. **NOTE**: This parameter is valid only when you select **Run once** on the Schedule tab.
Log Filter	
Include or exclude specific Logs	Use this parameter to filter the Logs you monitor. ◆ Select **Include only** to monitor only Logs that contain the descriptive text you provide in the *Failure log description text* parameter. ◆ Select **Exclude** to monitor all Logs except those that contain the descriptive text you provide in the *Failure log description text* parameter. The default is Exclude.
Failure log description text	Provide descriptive text that identifies the Logs you want to include in or exclude from monitoring, such as a location or an event ID.
Monitor Number of LINE Logs	
Event Notification	
Raise event if number of LINE logs exceeds threshold?	Select **Yes** to raise an event if the number of all LINE logs generated exceeds the threshold you set. The default is Yes. Enable this parameter to monitor all LINE logs: LINE101, LINE102, LINE104, LINE105, LINE115, LINE138, and LINE160. Use the LINE-specific parameters to monitor individual LINE logs.
Threshold - Maximum number of LINE logs	Specify the maximum number of LINE logs that can be generated before an event is raised. The default is 100 logs.
Event severity when number of LINE logs exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of LINE logs exceeds the threshold. The default is 15.

Parameter	How to Set It
Data Collection	
Collect data for number of LINE logs?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of LINE logs generated during the monitoring period. The default is Yes.
Monitor Number of LINE101 Logs	
Event Notification	
Raise event if number of LINE101 logs exceeds threshold?	Select **Yes** to raise an event if the number of LINE101 logs exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of LINE101 logs	Specify the maximum number of LINE101 logs that can be generated before an event is raised. The default is 100 logs.
Event severity when number of LINE101 logs exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of LINE101 logs exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of LINE101 logs?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of LINE101 logs generated during the monitoring period. The default is Yes.
Monitor Number of LINE102 Logs	
Event Notification	
Raise event if number of LINE102 logs exceeds threshold?	Select **Yes** to raise an event if the number of LINE102 logs exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of LINE102 logs	Specify the maximum number of LINE102 logs that can be generated before an event is raised. The default is 100 logs.
Event severity when number of LINE102 logs exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of LINE102 logs exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of LINE102 logs?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of LINE102 logs generated during the monitoring period. The default is Yes.
Monitor Number of LINE104 Logs	
Event Notification	
Raise event if number of LINE104 logs exceeds threshold?	Select **Yes** to raise an event if the number of LINE104 logs exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of LINE104 logs	Specify the maximum number of LINE104 logs that can be generated before an event is raised. The default is 100 logs.
Event severity when number of LINE104 logs exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of LINE104 logs exceeds the threshold. The default is 15.

Parameter	How to Set It
Data Collection	
Collect data for number of LINE104 logs?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of LINE104 logs generated during the monitoring period. The default is Yes.
Monitor Number of LINE105 Logs	
Event Notification	
Raise event if number of LINE105 logs exceeds threshold?	Select **Yes** to raise an event if the number of LINE105 logs exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of LINE105 logs	Specify the maximum number of LINE105 logs that can be generated before an event is raised. The default is 100 logs.
Event severity when number of LINE105 logs exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of LINE105 logs exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of LINE105 logs?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of LINE105 logs generated during the monitoring period. The default is Yes.
Monitor Number of LINE115 Logs	
Event Notification	
Raise event if number of LINE115 logs exceeds threshold?	Select **Yes** to raise an event if the number of LINE115 logs exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of LINE115 logs	Specify the maximum number of LINE115 logs that can be generated before an event is raised. The default is 100 logs.
Event severity when number of LINE115 logs exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of LINE115 logs exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of LINE115 logs?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of LINE115 logs generated during the monitoring period. The default is Yes.
Monitor Number of LINE138 Logs	
Event Notification	
Raise event if number of LINE138 logs exceeds threshold?	Select **Yes** to raise an event if the number of LINE138 logs exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of LINE138 logs	Specify the maximum number of LINE138 logs that can be generated before an event is raised. The default is 100 logs.
Event severity when number of LINE138 logs exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of LINE138 logs exceeds the threshold. The default is 15.

Parameter	How to Set It
Data Collection	
Collect data for number of LINE138 logs?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of LINE138 logs generated during the monitoring period. The default is Yes.
Monitor Number of LINE160 Logs	
Event Notification	
Raise event if number of LINE160 logs exceeds threshold?	Select **Yes** to raise an event if the number of LINE160 logs exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of LINE160 logs	Specify the maximum number of LINE160 logs that can be generated before an event is raised. The default is 100 logs.
Event severity when number of LINE160 logs exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of LINE160 logs exceeds the threshold. The default is 15.
Data Collection	
Collect data for number of LINE160 logs?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of LINE160 logs generated during the monitoring period. The default is Yes.

3.5 CallQuality

Use this Knowledge Script to monitor end-of-call voice quality statistics. This script raises an event when a monitored statistic exceeds or falls below the threshold you set. In addition, this script generates data streams for all monitored statistics. Event messages present call quality statistics for both legs of a call, from the sending and receiving phones, on a single line in the event detail, if data for both legs is available.

This script monitors the QoS Collector Application records that the CBM pushes to the QoS file collector service, as well as the QoS syslog records sent by the CICM Element Manager to the QoS syslog collector service:

MOS (Mean Opinion Score)

The quality of a VoIP transmission based on the "mouth-to-ear" characteristics of a speech path. A MOS of 5 is considered excellent. A MOS of 1 is unacceptably bad.

R-Value

Call quality value derived from delays and equipment impairment factors. An R-Value can be mapped to an estimated MOS. R-Values range from 100 (excellent) to 0 (poor).

Jitter

Also called delay variation, jitter is the mean deviation of the difference in packet spacing between the receiving phone and the sending phone.

Latency

The time taken for a packet of data to be sent by a phone, travel, and be received by another phone.

Packet loss

Percentage of packets lost or dropped between the sending and receiving phone.

NOTE: You can trigger NetIQ Vivinet Diagnostics to diagnose the problem when monitored voice quality statistics exceed the thresholds you set. For more information, see Section 3.16, "Triggering Call and Phone Quality Diagnoses," on page 67.

The purpose of this script is twofold:

- **Monitoring**. In monitoring mode, this script checks the database tables at each specified interval for new records that match your query. In the first iteration of the job, this script finds the last record in a table and checks back one interval from there. In subsequent iterations, this script checks for new records that match the query in each interval.
- **Troubleshooting**. In troubleshooting mode, this script runs once and checks the database tables for calls whose disconnect time is within the range you select in the *Select call disconnect time range* parameter. Select **Run once** on the Schedule tab to run this script in troubleshooting mode. AppManager does not collect call quality statistics unless this script is running, which could pose a problem should you want, for example, to troubleshoot a call that occurred five minutes ago. To perform troubleshooting as needed, also run CollectorHealth to start the collector services, which populate the Nortel CS2x supplemental database with data you can use for troubleshooting.

3.5.1 Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the supplemental database.
- Run CollectorHealth to start the QoS syslog collector service.

3.5.2 Resource Object

NortelCS2x IEMS

3.5.3 Default Schedule

By default, this script runs every five minutes.

3.5.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CallQuality job. The default is 5.
Raise event if data collector reports an error?	Select **Yes** to raise an event if the collector services report an error. The default is Yes. An error affects the entire data-collection connection and all data associated with that connection.

Parameter	How to Set It
Event severity when data collector reports an error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the collector services report an error. The default is 5.
Raise event if data collector reports a transaction error?	Select **Yes** to raise an event if the collector services report a transaction error. The default is Yes. A transaction error affects a single record encountered during the data-collection connection. If there are many transaction errors for the same record, only the most recent transaction error is posted for each iteration of the connection.
Event severity when data collector reports a transaction error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the collector services report a transaction error. The default is 10.
Raise event if data collector reports a warning?	Select **Yes** to raise an event if the collector services report a warning. The default is Yes.
Event severity when data collector reports a warning	Set the severity level, from 1 to 40, to indicate the importance of an event in which the collector services report a warning. The default is 15.
Include call details?	Select **Yes** to include call details in the events raised by this script. Leave this parameter unselected to suppress call details. When you select Yes, an event message includes the following columns: ◆ Listening Avg MOS ◆ Listening Avg R-Value ◆ Average Jitter (ms) ◆ Average Latency (ms) ◆ Lost Packets (%) ◆ Transmit Codec ◆ Receive Codec ◆ IP Address ◆ MAC Address ◆ Equipment ◆ Connect Time ◆ Disconnect Time ◆ Duration (seconds)
Maximum table size	If you selected Yes for *Include call details?*, specify the maximum number of rows of call detail to return in events raised by this script. The default is 25 rows.
Raise event if no records found?	Select **Yes** to raise an event if there are no call quality records to monitor in the Nortel CS2x supplemental database. Note that this does not mean there are no records with call quality data, but that there are no records at all. The default is unselected.
Event severity when no records found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no call quality records were found. The default is 25.
Monitor Settings	

Parameter	How to Set It
Perform traceroute and launch Vivinet Diagnostics when voice quality alert is received?	Select **Yes** to send a traceroute request to the CICM Element Manager and to launch Vivinet Diagnostics to diagnose the problem if vqalerts are received. The default is Yes.
Length of time to wait for traceroute responses	Specify the maximum length of time that the CallQuality job should wait for a response to traceroute requests to the CICM Element Manager. The CallQuality job will fail if the response time is longer than you specify. The default is 120 seconds.
Query Filters	No matter how many calls match the filters you select, an event message displays only the first 50 calls.
Minimum duration	Use this parameter to filter out records whose call duration is less than the value you specify. Accept the default of 0 seconds to ignore the filter for minimum duration.
Maximum duration	Use this parameter to filter out records whose call duration is greater than or equal to the value you specify. Accept the default of 0 seconds to ignore the filter for maximum duration.
Troubleshooting	
Select call disconnect time range	Select a **Specific** or **Sliding** date/time range for which the query should search for data. The default time range is fixed at 24 hours. **NOTE**: This parameter is valid only when you select **Run once** on the Schedule tab.
Monitor Average MOS	
Event Notification	
Raise event if average MOS falls below threshold?	Select **Yes** to raise an event if the average MOS value falls below the threshold you set. The default is Yes.
Threshold - Minimum average MOS	Specify the lowest average MOS value that must occur to prevent an event from being raised. The default is 3.60.
Event severity when average MOS falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average MOS value falls below the threshold you set. The default is 5.
Data Collection	
Collect data for average MOS?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average MOS value during the monitoring period. The default is unselected.
Monitor Average R-Value	
Event Notification	
Raise event if average R-Value falls below threshold?	Select **Yes** to raise an event if the average R-Value falls below the threshold you set. The default is Yes.
Threshold - Minimum average R-Value	Specify the lowest average R-Value that must occur to prevent an event from being raised. The default is 70.
Event severity when average R-Value falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average R-Value falls below the threshold. The default is 5.
Data Collection	

Parameter	How to Set It
Collect data for average R-Value?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average R-Value during the monitoring period. The default is unselected.
Monitor Average Jitter	
Event Notification	
Raise event if average jitter exceeds threshold?	Select **Yes** to raise an event if the average jitter value exceeds the threshold. The default is Yes.
Threshold - Maximum average jitter	Specify the highest average jitter value that can occur before an event is raised. The default is 60 milliseconds.
Event severity when average jitter exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average jitter value exceeds the threshold. The default is 15.
Data Collection	
Collect data for average jitter?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average amount of jitter that occurred during the monitoring period. The default is unselected.
Monitor Average Latency	
Event Notification	
Raise event if average latency exceeds threshold?	Select **Yes** to raise an event if the average latency value exceeds the threshold. The default is Yes.
Threshold - Maximum average latency	Specify the highest amount of average latency that can occur before an event is raised. The default is 400 milliseconds.
Event severity when average latency exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average latency value exceeds the threshold. The default is 15.
Data Collection	
Collect data for average latency?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the average amount of latency that occurred during the monitoring period. The default is unselected.
Monitor Average Packet Loss	
Event Notification	
Raise event if average packet loss exceeds threshold?	Select **Yes** to raise an event if the average packet loss value exceeds the threshold. The default is Yes.
Threshold - Maximum average packet loss	Specify the highest amount of average packet loss that can occur before an event is raised. The default is 1%.
Event severity when average packet loss exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the average packet loss value exceeds the threshold. The default is 15.
Data Collection	
Collect data for average packet loss?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of average packet loss that occurred during the monitoring period. The default is unselected.

3.6 CollectorHealth

Use this Knowledge Script to start the collector services and monitor their activity and availability. This script raises an event when a collector service is unavailable and when activity falls below the threshold you set. In addition, this script generates data streams for activity and availability of the following collector services:

- Log collector service, which receives logs from the IEMS
- OM file collector service, which receives OM Reports from the IEMS
- QoS file collector service, which receives end-of-call QoS Collector Application records from the CBM
- QoS syslog collector service, which receives syslogs from the CICM Element Manager

3.6.1 Prerequisites

- Configure the sFTP server user name and password in AppManager Security Manager. The OM and QoS syslog collector services receive data over secure FTP (sFTP). For more information, see Section 3.6.5, "Troubleshooting," on page 48.
- Run Discovery_NortelCS2x or SetupSupplementalDB to create the supplemental database.

3.6.2 Resource Object

NortelCS2x Data Collector

Run only one CollectorHealth job per data collector resource.

3.6.3 Default Schedule

By default, this script runs every five minutes.

3.6.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the CollectorHealth job. The default is 5.
Raise event if data collector reports an error?	Select **Yes** to raise an event if a collector service reports an error. The default is Yes. An error affects the entire data-collection connection and all data associated with that connection.
Event severity when data collector reports an error	Set the severity level, from 1 to 40, to indicate the importance of an event in which a collector service reports an error. The default is 5.

Parameter	How to Set It
Raise event if data collector reports a transaction error?	Select **Yes** to raise an event if a collector service reports a transaction error. The default is Yes. A transaction error affects a single record encountered during the data-collection connection. If there are many transaction errors for the same record, only the most recent transaction error is posted for each iteration of the connection.
Event severity when data collector reports a transaction error	Set the severity level, from 1 to 40, to indicate the importance of an event in which a collector service reports a transaction error. The default is 10.
Raise event if data collector reports a warning?	Select **Yes** to raise an event if a collector service reports a warning. The default is Yes.
Event severity when data collector reports a warning	Set the severity level, from 1 to 40, to indicate the importance of an event in which a collector service reports a warning. The default is 15.
Monitor Collector Availability	
Event Notification	
Raise event if collector service is unavailable?	Select **Yes** to raise an event if a collector service is unavailable. The default is Yes.
Event severity when collector service is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which a collector service is unavailable. The default is 5.
Data Collection	
Collect data for collector service availability?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns 0 if a collector service is unavailable and 100 if a collector service is available. The default is Yes.
Remediation	
Automatically start/restart collector service?	Select **Yes** to send a start request to a collector service. The start request allows the collector service to begin collecting data and populating the supplemental database. Data collection continues until the CollectorHealth job is stopped. If the collector service stops for any reason, it is restarted. The default is Yes. If you disable this parameter, the CollectorHealth job passively monitors collector service requests from other Knowledge Scripts. However, the CollectorHealth job does not request any data collection.
Monitor Collector Activity	
Event Notification	
Raise event if collector activity falls below threshold?	Select **Yes** to raise an event if collector service activity falls below the threshold you set. The default is Yes.
Threshold - Minimum collector activity	Specify the minimum number of transactions a collector service must perform to prevent an event from being raised. The default is 1 transaction per monitoring period.
Event severity collector activity falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which collector service activity falls below the threshold. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for collector activity?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of collector transactions during the monitoring period. The default is Yes.

3.6.5 Troubleshooting

Review the following topics for answers to questions you may have.

CollectorHealth Job Fails Password Authentication

Problem: The CollectorHealth job fails with the following error message:

```
Password authentication failed to <computer name>.
```

Cause: Most likely, the incorrect sFTP server user name and password are configured in AppManager Security Manager. The OM and QoS file collector services attempt to access the sFTP server using the user name and password configured in Security Manager. After *n* failed attempts (depending on how the switch is configured), the switch locks out the collector services and ignores subsequent login attempts.

Solution: Provide the correct user name and password in Security Manager. After the lockout expires, login succeeds and the CollectorHealth job runs successfully.

Log Collector Service Unavailable After a Power Outage

Problem: After a power outage, the CollectorHealth job raises an event indicating that the Log collector service is "unable to connect" to the IEMS.

Cause: Most likely, the IEMS service has not recovered from the power outage.

Solution: Verify the status of the IEMS service. If the service is down, issue the following command:

```
servstart iems
```

3.7 LogQuery

Use this Knowledge Script to monitor the number of logs in reports you specify. This script raises an event when the number of logs in the report exceeds the threshold you set.

This script uses the data collected by the log collector service.

The purpose of this script is twofold:

- **Monitoring**. In monitoring mode, this script checks the database tables at each specified interval for new records that match your query. In the first iteration of the job, this script finds the last record in a table and checks back one interval from there. In subsequent iterations, this script checks for new records that match the query in each interval.
- **Troubleshooting**. In troubleshooting mode, this script runs once and checks the database tables for calls whose disconnect time is within the range you select in the *Select call disconnect time range* parameter. Select **Run once** on the Schedule tab to run this script in troubleshooting mode. AppManager does not collect call quality statistics unless this script is running, which could pose a problem should you want, for example, to troubleshoot a call that occurred five minutes

ago. To perform troubleshooting as needed, also run CollectorHealth to start the collector services, which populate the Nortel CS2x supplemental database with data you can use for troubleshooting.

3.7.1 Monitoring Examples

The following table provides examples of report name and report number combinations you can use to monitor specific activities. Provide the report name in the *Report name* parameter and the report number in the *Report number* parameter.

Activity	Report	Number
Equipment down	PM	102
Equipment up	PM	106

3.7.2 Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the supplemental database.
- Run CollectorHealth to start the log collector service.

3.7.3 Resource Object

NortelCS2x IEMS

3.7.4 Default Schedule

By default, this script runs every five minutes.

3.7.5 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the LogQuery job fails. The default is 5.
Raise event if data collector reports an error?	Select **Yes** to raise an event if the log collector service reports an error. The default is Yes. An error affects the entire data-collection connection and all data associated with that connection.
Event severity when data collector reports an error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the log collector service reports an error. The default is 5.

Parameter	How to Set It
Raise event if data collector reports a transaction error?	Select **Yes** to raise an event if the log collector service reports a transaction error. The default is Yes. A transaction error affects a single record encountered during the data-collection connection. If there are many transaction errors for the same record, only the most recent transaction error is posted for each iteration of the connection.
Event severity when data collector reports a transaction error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the log collector service reports a transaction error. The default is 10.
Raise event if data collector reports a warning?	Select **Yes** to raise an event if the log collector service reports a warning. The default is Yes.
Event severity when data collector reports a warning	Set the severity level, from 1 to 40, to indicate the importance of an event in which the log collector service reports a warning. The default is 15.
Include details?	Select **Yes** to include log details in the events raised by this script. Leave this parameter unselected to suppress log details. When you select Yes, an event includes the following columns: ◆ Severity ◆ Report Name ◆ Report Number ◆ Report Time ◆ SequenceSS (a unique identifier for a log) ◆ SequenceDD (a unique identifier for a log) ◆ Event Type ◆ Event ID ◆ Report Details
Maximum table size	If you selected Yes for *Include details?*, specify the maximum number of rows of log detail that you want to return in events raised by this script. The default is 25 rows.
Troubleshooting	
Select log time range	Select a **Specific** or **Sliding** date/time range for which the query should search for data. The default time range is fixed at 24 hours. **NOTE**: This parameter is valid only when you select **Run once** on the Schedule tab.
Report name	Provide the name of the log report you want to query.
Report number	Provide the ID number of the log report you want to query.
Include or exclude specific reports	Select the filter to use when querying log reports. ◆ Select **Include only** to use only the log report specified in the *Log report description* parameter. ◆ Select **Exclude** to query for all log reports except the report specified in the *Log report description* parameter. The default is Exclude.

Parameter	How to Set It
Log report filter	
Log report description	Use this parameter to further filter the logs in the report you want to query. Provide a text explanation of the log you want to include or exclude from querying. An asterisk (*) is an acceptable wildcard. For example, to filter for any log that mentions a CICM, type `*CICM*`.
Monitor Number of Logs	
Event Notification	
Raise event if number of logs exceeds threshold?	Select **Yes** to raise an event if the number of logs in the specified report exceeds the threshold you set. The default is Yes.
Threshold - Maximum number of logs	Specify the maximum number of logs that can be in the specified report before an event is raised. The default is 100 logs.
Event severity when number of logs exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of logs in the specified report exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for number of logs?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the number of line logs found in the specified report. The default is Yes.

3.8 OMQuery

Use this Knowledge Script to monitor the value of a specified field in a specified table in an OM Report. This script raises an event when the value of the specified field exceeds the threshold you set.

This script uses the data collected by the OM file collector service.

The purpose of this script is twofold:

- **Monitoring**. In monitoring mode, this script checks the database tables at each specified interval for new records that match your query. In the first iteration of the job, this script finds the last record in a table and checks back one interval from there. In subsequent iterations, this script checks for new records that match the query in each interval.
- **Troubleshooting**. In troubleshooting mode, this script runs once and checks the database tables for calls whose disconnect time is within the range you select in the *Select call disconnect time range* parameter. Select **Run once** on the Schedule tab to run this script in troubleshooting mode. AppManager does not collect call quality statistics unless this script is running, which could pose a problem should you want, for example, to troubleshoot a call that occurred five minutes ago. To perform troubleshooting as needed, also run CollectorHealth to start the collector services, which populate the Nortel CS2x supplemental database with data you can use for troubleshooting.

3.8.1 Monitoring Examples

The following table provides examples of table/field name combinations you can use to monitor specific activities. Provide the table name in the *Table name* parameter and the field name in the *Field name* parameter.

Activity	Table	Field Name
Originating line calls	LMD	NTERMATT
Terminating line calls	LMD	NORIGATT
Outgoing trunk calls	OFZ	NORIG
Incoming trunk calls	OFZ	NIN
Blocked terminations: not enough channels or network resources to complete calls	LMD	TERMBLK
Blocked originations: not enough channels or network resources to originate calls	LMD	ORIGBLK
Blocked trunk calls	OFZ	TRMBLK
Failed originations, other than blocked: bad signaling, partial dial tone, bad dial tone	LMD	ORIGFAIL
Failed terminations, other than blocked	LMD	PERCLFL
Peripheral origination denied, device overload	PMOVLD	PORGDENY
Peripheral termination denied, device overload	PMOVLD	PTRMDENY
Calls lost due to equipment being down	PM	PMSBTCO

3.8.2 Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the supplemental database.
- Run CollectorHealth to start the OM file collector service.

3.8.3 Resource Object

NortelCS2x IEMS

3.8.4 Default Schedule

By default, this script runs every five minutes.

3.8.5 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	

Parameter	How to Set It
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the OMQuery job fails. The default is 5.
Raise event if data collector reports an error?	Select **Yes** to raise an event if the OM file collector service reports an error. The default is Yes. An error affects the entire data-collection connection and all data associated with that connection.
Event severity when data collector reports an error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the OM file collector service reports an error. The default is 5.
Raise event if data collector reports a transaction error?	Select **Yes** to raise an event if the OM file collector service reports a transaction error. The default is Yes. A transaction error affects a single record encountered during the data-collection connection. If there are many transaction errors for the same record, only the most recent transaction error is posted for each iteration of the connection.
Event severity when data collector reports a transaction error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the OM file collector service reports a transaction error. The default is 10.
Raise event if data collector reports a warning?	Select **Yes** to raise an event if the OM file collector service reports a warning. The default is Yes.
Event severity when data collector reports a warning	Set the severity level, from 1 to 40, to indicate the importance of an event in which the OM file collector service reports a warning. The default is 15.
Include details?	Select **Yes** to include OM Report details in the events raised by this script. Leave this parameter unselected to suppress details. When you select Yes, an event includes the following columns: ◆ NumFound ◆ Table Name ◆ Field Name ◆ Location
Maximum table size	If you selected Yes for *Include details?*, specify the maximum number of rows of detail that you want to return in events raised by this script. The default is 25 rows.
Troubleshooting	
Select OM time range	Select a **Specific** or **Sliding** date/time range for which the query should search for data. The default time range is fixed at 24 hours. **NOTE**: This parameter is valid only when you select **Run once** on the Schedule tab.
Table name	Provide the name of the table that you want to query in the OM Report.

Parameter	How to Set It
Field name	Provide the alpha-numeric identifier of the field in the table that you want to query. **Hints** ◆ When running this script in monitoring mode, provide only one field name for this parameter. ◆ When running this script in troubleshooting mode, leave this parameter blank.
Include or exclude specific locations	Select the IEMS systems for which you want to query OM Reports. ◆ Select **Include only** to query only the OM Reports from the system specified in the *Location* parameter. ◆ Select **Exclude** to query OM Reports for all systems except the system specified in the *Location* parameter. The default is Exclude.
Location	Provide the name of the IEMS system that you want to include or exclude from the querying of OM Reports.
Monitor OM Value	
Event Notification	
Raise event if value of OM Report exceeds threshold?	Set to **Yes** to raise an event if the value of the specified field in the OM Report exceeds the threshold you set. The default is Yes.
Threshold - Maximum value of OM Report	Indicate the maximum value allowed in the specified field in the OM Report. An event is raised if the value exceeds the threshold you set. The default is 100 units. **NOTE**: The value of the data stream generated by the script is a sum of the contents of all instances of the field you identified in the *Field name* parameter. AppManager applies the threshold to the data stream value.
Event severity when value of OM Report exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the value of the specified field in the OM Report exceeds the threshold you set. The default is 15.
Data Collection	
Collect data for value of OM Report?	Select **Yes** to collect data for charts and reports. When enabled, data collection returns the value of the specified field in the OM Report. The default is Yes.

3.9 PhoneDiagnostic

Use this Knowledge Script to invoke NetIQ Vivinet Diagnostics to diagnose call quality between the phone on which you run this script and another specified phone. This script's sole purpose is to invoke Vivinet Diagnostics on-demand, without waiting for a problem to be identified by the CallQuality or PhoneQuality Knowledge Script jobs.

This Knowledge Script job raises an event that launches the Action_DiagnoseVoIPQuality Knowledge Script, which in turn invokes Vivinet Diagnostics. For more information, see Section 3.16, "Triggering Call and Phone Quality Diagnoses," on page 67.

3.9.1 Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the Nortel CS2x supplemental database.
- Run CollectorHealth to start the QoS syslog collector service to populate the supplemental database with call quality data.
- Run RetrieveConfigData to populate the supplemental database with phone configuration data.
- Run AddPhone to add the phones you want to monitor to the AppManager console.

3.9.2 Resource Object

NortelCS2x Station Object

3.9.3 Default Schedule

By default, this script runs on an asynchronous schedule.

3.9.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the PhoneDiagnostic job fails. The default is 5.
Raise event if data collector reports an error?	Select **Yes** to raise an event if the QoS syslog collector service reports an error. The default is Yes. An error affects the entire data-collection connection and all data associated with that connection.
Event severity when data collector reports an error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the QoS syslog collector service reports an error. The default is 10.
Raise event if data collector reports a warning?	Select **Yes** to raise an event if the QoS syslog collector service reports a warning. The default is Yes.
Event severity when data collector reports a warning	Set the severity level, from 1 to 40, to indicate the importance of an event in which the QoS syslog collector service reports a warning. The default is 15.
Monitor Settings	
Length of time to wait for traceroute responses	Specify the maximum length of time that the PhoneDiagnostic job should wait for a response to traceroute requests to the CICM Element Manager. The PhoneDiagnostic job will fail if the response time is longer than you specify. The default is 120 seconds.
Far End (Remote) Phone Settings	
Select remote phone by	Select the category by which you want to choose the phone you want to monitor. Select **Terminal**, **DN**, or **IPAddress**. The default is DN.

Parameter	How to Set It
Selection criteria	Based on your selection in *Select remote phone by*, provide details for the phone you want to monitor. Vivinet Diagnostics diagnoses call quality between this phone and the phone on which you run this script. ◆ *If you selected Terminal*, provide the terminal address of the phone you want to monitor. ◆ *If you selected DN*, provide the Directory Number of the phone you want to monitor ◆ *If you selected IPAddress*, provide the IP address of the phone you want to monitor.

3.10 PhoneInventory

Use this Knowledge Script to create an inventory of the phones configured for a CICM Element Manager.

You choose both the search criteria for the inventory report and the location of the output folder. The inventory report is written to the computer on which the AppManager agent is running, unless you specify a UNC path: `\\servername\sharename\directoryname\filename`. If you specify a UNC path, ensure the `NetIQmc` service is running as an account that has proper permissions on the UNC path.

3.10.1 Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the supplemental database.
- Run RetrieveConfigData to populate the supplemental database with phone configuration information.

3.10.2 Resource Object

NortelCS2x

3.10.3 Default Schedule

By default, this script runs once.

3.10.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the PhoneInventory job fails. The default is 5.

Parameter	How to Set It
Raise event if phone inventory succeeds?	Select **Yes** to raise an event when a phone inventory report is successfully generated. The default is Yes.
Event severity when phone inventory succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a phone inventory report is successfully generated. The default is 25.
Raise event if no records found?	Set to **Yes** to raise an event when the PhoneInventory job finds no phones based on the criteria you selected. The default is Yes
Event severity when no records found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the PhoneInventory job found no phones based on the criteria you selected. The default is 25.
Search Options	
Select phones by	Select the filter by which you want to select the phones for the inventory report. Choose one of the following: ◆ Node ◆ Terminal ◆ DN (Directory Number, the default) ◆ Station Type ◆ Network Name ◆ Network ID ◆ IP Address
Selection criteria	Provide the selection criteria for the phones to include in the inventory report. You can specify the actual item or you can specify a pattern by using the * wildcard. For example, to monitor all the phones in the ADM building, type `ADM*`. You can enter multiple criteria by separating each item with a comma. For example: `ADM0009A*,ADM0009B*` The criteria you enter must be of the same type as the *Select phones by* parameter. So if *Select phones by* is Terminal, then the criteria must be terminal names or patterns. If *Select phones by* is DN, then the criteria must be phone extension numbers. **NOTE**: Only the following characters are acceptable in this field: ◆ Numbers ◆ Uppercase and lowercase letters ◆ Periods ◆ Commas ◆ Asterisks (*) ◆ Underscores ◆ Spaces

Parameter	How to Set It
List only phones with status of	To further filter the list of phones, select a status. Only phones of this status type, matching the criteria you specified in *Selection criteria* and *Select phones by*, are included in the inventory report. Choose one of the following: ◆ Any ◆ Logged In ◆ Logged Out
Result File Options	
Full path to output folder for result file	Type the full path or a UNC path to a location on the agent computer in which to save the inventory .csv file. The default path is `c:\Program Files\NetIQ\Temp\NetIQ_Debug\PhoneInventory.csv`
Sort by	Select **Name** to sort the contents of the inventory report in order by phone name, specifically by the "node" column and then by the "terminalid" column. Select **DN** to sort the contents of the inventory report in order by Directory Number, specifically by the "ud_pDN" column (Primary Directory Number) column. The default is DN.

3.11 PhoneQuality

Use this Knowledge Script to monitor real-time voice quality statistics from active calls on IP phones. This script raises one event per call if monitored statistics exceed or fall below the threshold you set. In addition, this script generates data streams for each monitored statistic.

This script monitors the mid-call QoS records for the Phase 2 IP phones on which you run this script. The QoS syslog collector service receives those records from the Call Server and pushes those records to the supplemental database.

MOS (Mean Opinion Score)

Represents the quality of a VoIP transmission by factoring in the "mouth-to-ear" characteristics of a speech path. A MOS of 5 is considered excellent; a MOS of 1 is unacceptably bad.

R-Value

Call quality value derived from delays and equipment impairment factors. An R-Value can be mapped to an estimated MOS. R-Values range from 100 (excellent) to 0 (poor).

Jitter

Also called delay variation, jitter is the mean deviation of the difference in packet spacing between the calling phone and the called phone.

Latency

The time taken for a data packet to be sent by a phone, travel, and be received by another phone.

Packet loss

Packets lost or dropped between the calling and called phone

NOTE: You can trigger NetIQ Vivinet Diagnostics to diagnose the problem when monitored voice quality statistics exceed the thresholds you set. For more information, see Section 3.16, "Triggering Call and Phone Quality Diagnoses," on page 67.

3.11.1 Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the Nortel CS2x supplemental database.
- Run RetrieveConfigData to populate the supplemental database with phone configuration data.
- Run AddPhone to add the phones you want to monitor to the AppManager console.
- Run CollectorHealth to start the QoS syslog collector service.

3.11.2 Resource Object

NortelCS2x Station Object

3.11.3 Default Schedule

By default, this script runs on an asynchronous schedule.

3.11.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the PhoneQuality job. The default is 5.
Raise event if data collector reports an error?	Select **Yes** to raise an event if the QoS syslog collector service reports an error. The default is Yes. An error affects the entire data-collection connection and all data associated with that connection.
Event severity when data collector reports an error	Set the severity level, from 1 to 40, to indicate the importance of an event in which the QoS syslog collector service reports an error. The default is 10.
Raise event if data collector reports a warning?	Select **Yes** to raise an event if the QoS syslog collector service reports a warning. The default is Yes.
Event severity when data collector reports a warning	Set the severity level, from 1 to 40, to indicate the importance of an event in which the QoS syslog collector service reports a warning. The default is 15.
Monitor Settings	
Data collection interval for voice quality metrics	Specify how often the PhoneQuality script should collect phone quality statistics from the supplemental database. The default is 30 seconds, the minimum is 15 seconds, and the maximum is 1000000 seconds.

Parameter	How to Set It
Perform traceroute and launch Vivinet Diagnostics when voice quality alert is received?	Select **Yes** to send a traceroute request to the CICM Element Manager and to launch Vivinet Diagnostics to diagnose the problem if vqalerts are received. The default is Yes.
Length of time to wait for traceroute responses	Specify the maximum length of time that the PhoneQuality job should wait for a response to traceroute requests to the CICM Element Manager. The PhoneQuality job will fail if the response time is longer than you specify. The default is 120 seconds.
Monitor Interval MOS	
Event Notification	
Raise event if interval MOS falls below threshold?	Select **Yes** to raise an event if the MOS value during the data collection interval falls below the threshold you set. The default is Yes.
Threshold - Minimum interval MOS	Specify the minimum MOS value that must occur during the data collection interval to prevent an event from being raised. The default is 3.60.
Event severity when interval MOS falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the MOS value during the data collection interval falls below the threshold. The default is 5.
Data Collection	
Collect data for interval MOS?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the MOS value during the data collection period. The default is Yes.
Monitor Interval R-Value	
Event Notification	
Raise event if interval R-Value falls below threshold?	Select **Yes** to raise an event if the R-Value during the data collection interval falls below the threshold you set. The default is Yes.
Threshold - Minimum interval R-Value	Specify the lowest R-Value that must occur during the data collection interval to prevent an event from being raised. The default is 70.
Event severity when interval R-Value falls below threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the R-Value during the data collection interval falls below the threshold. The default is 5.
Data Collection	
Collect data for interval R-Value?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the R-Value during the data collection interval. The default is unselected.
Monitor Interval Jitter	
Event Notification	
Raise event if interval jitter exceeds threshold?	Select **Yes** to raise an event if the jitter value during the data collection interval exceeds the threshold you set. The default is Yes.
Threshold - Maximum interval jitter	Specify the highest jitter value that can occur during the data collection interval before an event is raised. The default is 60 milliseconds.
Event severity when jitter exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the jitter value exceeds the threshold. The default is 15.
Data Collection	

Parameter	How to Set It
Collect data for interval jitter?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of jitter that occurred during the data collection interval. The default is unselected.
Monitor Interval Latency	
Event Notification	
Raise event if interval latency exceeds threshold?	Select **Yes** to raise an event if the latency value during the data collection interval exceeds the threshold you set. The default is Yes.
Threshold - Maximum interval latency	Specify the highest amount of latency that can occur during the data collection interval before an event is raised. The default is 400 milliseconds.
Event severity when interval latency exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the latency value during the data collection interval exceeds the threshold. The default is 15.
Data Collection	
Collect data for interval latency?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the amount of latency that occurred during the data collection interval. The default is unselected.
Monitor Interval Packet Loss	
Event Notification	
Raise event if interval packet loss exceeds threshold?	Select **Yes** to raise an event if the packet loss value during the data collection interval exceeds the threshold. The default is Yes.
Threshold - Maximum interval packet loss	Specify the highest percentage of packet loss that can occur during the data collection interval before an event is raised. The default is 1%.
Event severity when interval packet loss exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the packet loss value during the data collection interval exceeds the threshold. The default is 15.
Data Collection	
Collect data for interval packet loss?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the percentage of packet loss that occurred during the monitoring period. The default is unselected.

3.12 RemovePhone

Use this Knowledge Script to remove IP phones (stations) from the AppManager console. This Knowledge Script is not available for use if you never used AddPhone to add an IP station.

When this Knowledge Script job runs successfully, the resource object for an IP station is deleted from the AppManager console. The job itself is not deleted, nor is the event that the job creates because the event is associated with the parent object: `NortelCS2x:<`*computer name*`>` object. However, you can set a global preference to ensure that an event is deleted when the associated object is deleted.

To delete associated events:

1 From the File menu, select **Preferences**.

2 Click **Repository**, and then click **Event**.

3 Select **Remove associated events when jobs are deleted**.

TIP

- When you run this script, verify your selected phones in the Objects tab to avoid removing a phone that you want to keep.
- Before attempting to remove a phone, stop any monitoring jobs that are running on the phone.

3.12.1 Resource Object

NortelCS2x Station Object

3.12.2 Default Schedule

By default, this script runs once.

3.12.3 Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of the failure of the RemovePhone job. The default is 5.
Event Notification	
Raise event if phones are removed successfully?	Select **Yes** to raise an event if the selected IP stations are successfully removed from AppManager console. The default is Yes.
Event severity when phones are removed successfully	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the selected IP stations are successfully removed from the AppManager console. The default is 25.

3.13 RetrieveConfigData

Use this Knowledge Script to retrieve station configuration information from individual CICM Element Managers. This script stores the configuration information in the Nortel CS2x supplemental database, where it can be monitored by the PhoneInventory and PhoneDiagnostic Knowledge Scripts.

3.13.1 Prerequisites

- Run Discovery_NortelCS2x or SetupSupplementalDB to create the supplemental database.
- Configure the CICM Element Manager user name and password in AppManager Security Manager. For more information, see Section 2.9.1, “Configuring CICM User Names and Passwords,” on page 26.

3.13.2 Resource Object

NortelCS2x

3.13.3 Default Schedule

By default, this script runs once every day at 3 AM, so as to perform CPU-intensive functions at a time when Element Managers are least busy.

To populate the supplemental database immediately, change the schedule to **Run Once**.

3.13.4 Setting Parameter Values

Set the following parameters as needed:

Description	How To Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of the failure of the RetrieveConfigData job. The default is 5.
Raise event if configuration retrieval succeeds?	Select **Yes** to raise an event if the RetrieveConfigData job successfully stores station configuration information in the Nortel CS2x supplemental database. The default is unselected.
Event severity when configuration retrieval succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which configuration information is successfully stored in the NortelCS2x supplemental database. The default is 25.

3.14 SetupSupplementalDB

Use this Knowledge Script to create the Nortel CS2x supplemental database, including the tables and stored procedures needed to store logs, OM Reports, QoS and call detail records, and station configuration information. In addition, this script creates a SQL Server job that removes old records from the supplemental database.

When you create the supplemental database, you specify how long data is retained before being deleted. AppManager automatically deletes any records older than the retention age you specify.

3.14.1 Understanding the Supplemental Database

The Nortel CS2x supplemental database is a Microsoft SQL Server database you create locally on the proxy agent computer or on a specified remote computer. The log, OM, QoS syslog, and QoS file collector services receive data from the IEMS, the CICM, the CBM, and the Call Server, and then store that data in the supplemental database.

- The CollectorHealth Knowledge Script verifies that collectors are receiving data and starts the process by which the collectors push their data to the supplemental database.

- The CallActivity, CallFailures, CallQuality, LogQuery, and OMQuery, and PhoneQuality Knowledge Scripts query the supplemental database for the data you specify.
- The RetrieveConfigData Knowledge Script populates the supplemental database with station information used by the PhoneInventory and PhoneDiagnostic Knowledge Scripts.

To create and use the supplemental database:

1. **Create the database**. Create one Nortel CS2x supplemental database per office supported by a Communication Server solution. You can create the supplemental database when you run Discovery_NortelCS2x or SetupSupplementalDB.
2. **Populate the database**. Run CollectorHealth and RetrieveConfigData to populate the Nortel CS2x supplemental database.
3. **Monitor the data in the database**. Depending on your monitoring objectives, run the following scripts to analyze the data in the database.
   - CallActivity monitors active and completed calls.
   - CallFailures monitors LINE (line maintenance) logs.
   - CallQuality monitors end-of-call voice quality statistics: jitter, latency, lost data, MOS, and R-Value.
   - LogQuery monitors logs in specified log reports.
   - OMQuery monitors specified fields in the OM Report.
   - PhoneDiagnostic invokes NetIQ Vivinet Diagnostics to diagnose call quality between two phones.
   - PhoneInventory creates an inventory of the phones configured in a CICM Element Manager.
   - PhoneQuality monitors real-time, mid-call voice quality statistics from active calls on IP phones.

3.14.2 Resource Object

NortelCS2x IEMS

3.14.3 Default Schedule

By default, this script runs once.

3.14.4 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the failure of the SetupSupplementalDB job. The default is 5.
Raise event if database setup succeeds?	Select **Yes** to raise an event if creation of the Nortel CS2x supplemental database is successful. The default is unselected.

Parameter	How to Set It
Event severity when database setup succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the success of the creation of the Nortel CS2x supplemental database. The default is 25.
Number of days to keep supplemental database records	Specify the number of days you want to keep records in the Nortel CS2x supplemental database. Data older than that is discarded. The default is 14 days.
SQL Server computer name	Specify the hostname or IP address of the remote SQL Server computer on which you want to create the Nortel CS2x supplemental database. Leave this parameter blank to create the supplemental database on the proxy agent (local) computer. For either a remote or local supplemental database, configure the SQL Server user name and password in AppManager Security Manager. For more information, see Section 2.9.3, “Configuring SQL Server User Names and Passwords,” on page 27. For a remote supplemental database, set up the remote SQL Server computer. For more information, see Section 2.10, “Configuring the Remote Supplemental Database Computer,” on page 27.
SQL Server instance name	Specify the name of the SQL Server instance on the computer on which you want to create the Nortel CS2x supplemental database. Leave this parameter blank to accept the default instance name.

Parameter	How to Set It
Start pruning job on supplemental database?	**For all supported versions of SQL Server, except SQL Server 2005 Express**: Set to **Yes** to create a SQL job that deletes data from the supplemental database. The SQL job runs every night. Data is deleted from the supplemental database based on the value you specify in the *Number of days to keep call detail records* parameter. The default is Yes. **For SQL Server 2005 Express**: Set to **No**. The pruning job is not supported for SQL Server 2005 Express. **To manually delete data from the supplemental database**: 1. Run the following stored procedure from a command line: `osql -E -S <sql server> -n -d <database> -Q "exec dbo.Task_NortelCS2x_Pruning"` where `<sql server>` is the name of the server that hosts the supplemental database, and where `<database>` is the name of the supplemental database. For example: `osql -E -S SuppDBNortelCS2x -n -d NortelCS2x_S8300-Cluster -Q "exec dbo.Task_NortelCS2x_Pruning"` 2. Configure a Windows Scheduled Task to schedule pruning at an interval of your choosing. The process for configuring a Windows Scheduled Task varies according to your version of Microsoft Windows. Consult your Windows documentation for more information.

3.15 Recommended Knowledge Script Group

The following Knowledge Scripts in the AppManager for Nortel CS2x module are members of the NortelCS2x recommended Knowledge Script Group (KSG).

- CallActivity
- CallFailures
- CallQuality
- CollectorHealth

You can find the NortelCS2x KSG on the RECOMMENDED tab of the Knowledge Script pane of the Operator Console.

All the scripts in the KSG have their parameters set to recommended values. To run all of the recommended scripts at one time, click the RECOMMENDED tab, and then run the NortelCS2x group on a Nortel CS2x resource.

Run the KSG from the Master view, not the NortelCS2x view. In order to use the Discovery_NortelCS2x Knowledge Script in a monitoring policy, the view must include root objects, which are not visible in the NortelCS2x view.

The NortelCS2x KSG enables a "best practices" usage of AppManager for monitoring your Nortel CS2x environment. You can use this KSG with AppManager monitoring policies. A monitoring policy, which enables you to efficiently and consistently monitor all the resources in your environment, uses a set of pre-configured Knowledge Scripts to automatically monitor resources as they appear in the TreeView. For more information, see "About Policy-Based Monitoring" in the AppManager Help.

A KSG is composed of a subset of a module's Knowledge Scripts. The script that belongs to a KSG is a different copy of the original script you access from the NortelCS2x tab. If you modify a script that belongs to a KSG, the parameter settings of the original script in the NortelCS2x tab are not affected.

In some cases, default script parameter settings are different when the script is deployed as part of a KSG, as opposed to when it is deployed alone. The default settings of a script within a group depend on its monitoring purpose within the larger group, and on the intended monitoring scope of that group.

If you modify or remove a script associated with the NortelCS2x KSG and want to restore it to its original form, you can reinstall AppManager for Nortel CS2x on the repository computer or check in the appropriate script from the `AppManager\qdb\kp\NortelCS2x` directory.

3.16 Triggering Call and Phone Quality Diagnoses

You can use NetIQ Vivinet Diagnostics to diagnose problems identified by NortelCS2x Knowledge Scripts.

Using the existing methodology of launching an Action script based on an event, AppManager can launch Action_DiagnoseVoIPQuality to trigger Vivinet Diagnostics in the following instances. The Action script runs by default only if Vivinet Diagnostics 2.3 or later is installed on the computer on which the script is running.

- To diagnose the problem for events raised by the CallQuality and PhoneQuality Knowledge Scripts.
- You can use the PhoneDiagnostic Knowledge Script to trigger Vivinet Diagnostics on demand, rather than waiting for a problem to be identified by the CallQuality and PhoneQuality Knowledge Scripts.

You can also use the CallAlert Knowledge Script to trigger Vivinet Diagnostics to diagnose the problems indicated by vqalerts.

To trigger Vivinet Diagnostics:

1. When setting parameter values for the CallQuality, PhoneQuality, or PhoneDiagnostic Knowledge Scripts, click the **Action** tab. Action_DiagnoseVoIPQuality is selected by default.
2. Click **Properties** and enter values for all parameters for Action_DiagnoseVoIPQuality.
3. Click **OK** to run the CallQuality, PhoneQuality, or PhoneDiagnostic Knowledge Script jobs.

The event message for the Action_DiagnoseVoIPQuality job provides a hyperlink to a .dgv file, which is the Diagnosis. Click the link to view the Diagnosis in the Vivinet Diagnostics console. For more information, see the *User Guide for Vivinet Diagnostics* and the Help for the Action_DiagnoseVoIPQuality Knowledge Script.