Management Guide

NetIQ® AppManager® for Microsoft Active Directory

July 2019

Legal Notice

Contents

About this Book and the Library

The NetIQ AppManager for Microsoft Active Directory 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 Microsoft Active Directory provides system administrators with a central, easy-to-use console to view critical server and application resources across the enterprise. With AppManager for Microsoft Active Directory, 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 s, 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 Microsoft Active Directory library is available in Adobe Acrobat (PDF) format from the AppManager Documentation page of the NetIQ Web site.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

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

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, 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, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also 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, visit http://community.netiq.com.

1 Introducing AppManager for Active Directory

Active Directory allows you to organize and manage your Windows network and directory resources. Active Directory is a directory service included with most Microsoft Windows Server operating systems.

This chapter summarizes the ways AppManager can help you monitor Active Directory.

1.1 Why Monitor Active Directory?

The following are a few reasons that proper monitoring of Active Directory should be a top priority:

- The root-cause of Active Directory problems are easy to detect and repair early, but are difficult to diagnose and repair later.
- Most Active Directory problems can cause logon problems for entire sites within a company, or even for multiple sites.
- Some Active Directory problems are so severe that starting over with a clean installation may be necessary.
- About half of Exchange connectivity and performance issues are actually Active Directory issues.
- Active Directory health is difficult to determine because it relies on the interaction of many technologies, including File Replication Service (FRS), Netlogon, Lightweight Directory Access Protocol (LDAP), and Kerberos.
- Active Directory replication becomes exponentially more complex with each additional Active Directory server.

Despite the complexity of Active Directory, close management of each of its sub-functions or components is not necessary. Nor must you examine the thousands of event log messages that are generated daily.

1.2 How AppManager Can Help

NetIQ Corporation offers a monitoring system based on a solid understanding of Active Directory and many years of experience managing it at customer sites. NetIQ Corporation has created a set of general guidelines as well as minimum recommended and best monitoring practices. This guide provides instructions and advice for following these guidelines and using the recommended AD Knowledge Script Groups in a way that best suits your unique Active Directory installation.

With AppManager, you can monitor and manage the following:

- Core health of key Active Directory components, including Flexible Single Master Operations (FSMOs), replication, trusts, Kerberos, Timesync, NetLogon, FRS, and SysVol.
- CPU utilization, memory consumption, and key performance counters.
- Replication latency for all Active Directory partitions.
- Interface health for LDAP and global catalogs.

- Any Active Directory-related entries in the Windows Event Log.
- The number of objects and other specific Active Directory components.
- Interrelated groups of servers with changing roles that need selective Knowledge Script execution. You can use job delegation to accomplish this task.

A set of *Knowledge Script Groups* is provided to help you run jobs right out of the box while still adhering to NetIQ Corporation best practice guidelines for monitoring Microsoft Active Directory. These collections of Knowledge Scripts from the AD category have been grouped to perform common monitoring functions. Some Knowledge Scripts within a Knowledge Script Group have different default settings to help the group perform a particular function.

For more information, see Section 3.48, “AD Knowledge Script Groups,” on page 107. Knowledge Script Groups are available on the RECOMMENDED tab in the Operator Console Knowledge Script pane.

You can best use Knowledge Script Groups by employing AppManager monitoring policies in your environment. For more information, see “About Policy-Based Monitoring” in the AppManager Help.

2 Installing AppManager for Active Directory

This chapter provides installation instructions and describes system requirements for AppManager for Microsoft Active Directory:

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 page.

2.1 System Requirements

For the latest information about supported software versions and the availability of module updates, visit the AppManager Supported Products page. Unless noted otherwise, this module supports all updates, hotfixes, and service packs for the releases listed below.

AppManager for Active Directory has the following system requirements:

Software/Hardware	Version
NetIQ AppManager installed on the AppManager repository (QDB) computers, on the Active Directory computers you want to monitor (agents), and on all console computers	8.0.3, 8.2, 9.1, 9.2, 9.5, or later One of the following AppManager agents are required: ◆ AppManager agent 7.0.4 with hotfix 72616 or later ◆ AppManager agent 8.0.3, 8.2, 9.1, 9.2, 9.5, or later
Microsoft Windows operating system on the agent computers	One of the following: ◆ Windows Server 2019 ◆ Windows Server 2016 ◆ Windows Server 2012 ◆ Windows Server 2008 R2 ◆ Windows Server 2008 (32-bit or 64-bit) ◆ Windows Server 2003 R2 (32-bit or 64-bit) ◆ Windows Server 2003 (32-bit or 64-bit)
AppManager for Microsoft Windows module installed on the AppManager repository (QDB) computer, on the Active Directory computers you want to monitor (agents), and on all console computers	Support for Windows Server 2008 R2 on AppManager 7.x requires the AppManager for Windows module, version 7.6.170.0 or later. For more information, see the AppManager Module Upgrades & Trials Web page.
Microsoft SQL Server Native Client 11.0 **(for TLS 1.2 support)**	11.3.6538.0 or later **NOTE:** The SQL Server Native client can be installed from this Microsoft download link.

If you encounter problems using this module with a later version of your application, contact NetIQ Technical Support.

NOTE: If you want TLS 1.2 support and are running AppManager 9.1 or 9.2, then you are required to perform some additional steps. To know about the steps, see the article.

2.2 Installing the Module

Run the module installer only once on any computer. The module installer automatically identifies and updates all relevant AppManager components on a computer.

Access the `AM70-AD-7.x.x.0.msi` module installer from the `AM70_AD_7.x.x.0` self-extracting installation package on the AppManager Module Upgrades & Trials page.

For Windows environments where User Account Control (UAC) is enabled, install the module using an account with administrative privileges. Use one of the following methods:

- Log in to the server using the account named Administrator. Then, run `AM70-AD-7.x.x.0.msi` from a command prompt or by double-clicking it.
- Log in to the server as a user with administrative privileges and run `AM70-AD.x.x.0.msi` as an administrator from a command prompt. To open a command-prompt window at the administrative level, right-click a command-prompt icon or a Windows menu item and select **Run as administrator**.

You can install the Knowledge Scripts and the Analysis Center reports into local or remote AppManager repositories (QDBs). Install these components only once per QDB.

The module installer now installs Knowledge Scripts for each module directly into the QDB instead of installing the scripts in the `\AppManager\qdb\kp` folder as in previous releases of AppManager.

You can install the module manually, or you can use Control Center to deploy the module on a remote computer where an agent is installed. For more information, see Section 2.3, “Deploying the Module with Control Center,” on page 13. However, if you use Control Center to deploy the module, Control Center only installs the *agent* components of the module. The module installer installs the QDB and console components as well as the agent components on the agent computer.

To install the module manually:

1. Double-click the module installer `.msi` file.
2. Accept the license agreement.
3. Review the results of the pre-installation check. You can expect one of the following three scenarios:
   - **No AppManager agent is present:** In this scenario, the pre-installation check fails, and the installer does not install agent components.
   - **An AppManager agent is present, but some other prerequisite fails:** In this scenario, the default is to not install agent components because of one or more missing prerequisites. However, you can override the default by selecting Install agent component locally. A missing application server for this particular module often causes this scenario. For example, installing the AppManager for Microsoft SharePoint module requires the presence of a Microsoft SharePoint server on the selected computer.
   - **All prerequisites are met:** In this scenario, the installer installs the agent components.

4 To install the Knowledge Scripts into the QDB and to install the Analysis Center reports into the Analysis Center Configuration Database:

   4a Select **Install Knowledge Scripts** to install the repository components, including the Knowledge Scripts, object types, and SQL stored procedures.

   4b Select **Install report package** to install the Analysis Center reports.

   4c Specify the SQL Server name of the server hosting the QDB, as well as the case-sensitive QDB name.

   4d Specify the SQL Server name of the server hosting the Analysis Center Configuration Database.

5 (Conditional) If you use Control Center 7.x, run the module installer for each QDB attached to Control Center.

6 (Conditional) If you use Control Center 8.x or later, run the module installer only for the primary QDB. Control Center automatically replicates this module to secondary QDBs.

7 Run the module installer on all console computers to install the Help and console extensions.

8 Run the module installer on the Active Directory computers you want to monitor (agents) to install the agent components.

9 (Conditional) If you have not discovered Active Directory resources, run the Discovery_ActiveDS Knowledge Script on all agent computers where you installed the module. For more information, see Section 2.6, “Discovering Active Directory Resources,” on page 15.

10 To get the updates provided in this release, upgrade any running Knowledge Script jobs. For more information, see Section 2.7, “Upgrading Knowledge Script Jobs,” on page 21.

After the installation has completed, the `AD_Install.log` file, located in the `\NetIQ\Temp\NetIQ_Debug\`*`ServerName`* folder, lists any problems that occurred.

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 page.

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. For more information, see Section 2.3.2, “Checking In the Installation Package,” on page 14.

3 Configure an e-mail 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-AD-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 using an account that is a member of a user group with deployment permissions.
2. Navigate to the **Deployment** tab (for AppManager 8.x or later) or **Administration** tab (for AppManager 7.x).
3. In the Deployment folder, select **Packages**.
4. On the Tasks pane, click **Check in Deployment Packages** (for AppManager 8.x or later) or **Check in Packages** (for AppManager 7.x).
5. Navigate to the folder where you saved `AM70-AD-7.x.x.0.xml` and select the file.
6. Click **Open**. The Deployment Package Check in Status dialog box displays the status of the package check in.
7. To get the updates provided in this release, upgrade any running Knowledge Script jobs. For more information, see Section 2.7, “Upgrading Knowledge Script Jobs,” on page 21.

2.4 Silently Installing the Module

To silently (without user intervention) install a module using the default settings, run the following command from the folder in which you saved the module installer:

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

where *x.x* is the actual version number of the module installer.

To get the updates provided in this release, upgrade any running Knowledge Script jobs. For more information, see Section 2.7, “Upgrading Knowledge Script Jobs,” on page 21.

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

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

The log file is created in the folder in which you saved the module installer.

NOTE: To perform a silent install on an AppManager agent running Windows Server 2012 or Windows Server 2008 R2, open a command prompt at the administrative level and select **Run as administrator** before you run the silent install command listed above.

To silently install the module on a remote AppManager repository, you can use Windows authentication or SQL authentication.

Windows authentication:

```
AM70-AD-7.x.x.0.msi /qn MO_B_QDBINSTALL=1 MO_B_MOINSTALL=0 MO_B_SQLSVR_WINAUTH=1
MO_SQLSVR_NAME=SQLServerName MO_QDBNAME=AM-RepositoryName
```

SQL authentication:

```
AM70-AD-7.x.x.0.msi /qn MO_B_QDBINSTALL=1 MO_B_MOINSTALL=0 MO_B_SQLSVR_WINAUTH=0
MO_SQLSVR_USER=SQLLogin MO_SQLSVR_PWD=SQLLoginPassword
MO_SQLSVR_NAME=SQLServerName MO_QDBNAME=AM-RepositoryName
```

2.5 Permissions for Running Knowledge Scripts

AppManager for Active Directory requires that the NetIQ AppManager Client Resource Monitor (`netiqmc`) and the NetIQ AppManager Client Communication Manager (`netiqccm`) agent services have the following permissions:

- Ability to log on as a service
- Membership in the Domain Admin Group

By default, the module installer configures the agent to use the Windows Local System account.

To update the agent services:

1. Start the Services Administrative Tool. You can open the Administrative Tools folder in the Control Panel.
2. Right-click the **NetIQ AppManager Client Communication Manager** (`netiqccm`) service in the list of services, and select **Properties**.
3. On the Logon tab, specify the appropriate account to use.
4. Click **OK**.
5. Repeat steps 2 through 4 for the **NetIQ AppManager Client Resource Monitor** (`netiqmc`) service.
6. Restart both services.

2.6 Discovering Active Directory Resources

Use the Discovery_ActiveDS Knowledge Script to discover Active Directory servers and resources for Windows Server operating systems. For more information about specific operating systems, see Section 2.1, “System Requirements,” on page 11. You can display the server name and the roles for the server, such as FSMO and Global Catalog.

Because the number of network computer objects stored in the Active Directory tree can be large, you can limit the number of Domain Naming Context and Configuration Container objects that are discovered:

- Specify the container level depth for discovery. Only container levels that are within the specified level of the domain tree are discovered.
- Specify the number of child objects to discover within a container level.
- Specify the particular classes of objects you want to include or exclude for discovery. The option of selecting the objects to include or exclude, however, depends on which version of AppManager for Microsoft Active Directory you are using.
- Specify whether to limit discovery to domains that have a direct trust relationship to the domain where discovery is performed, to domains that are in the same forest, or to Active Directory domains.

Depending on the version of the AppManager for Microsoft Active Directory agent on the Active Directory server, you can specify the objects you want to discover by excluding or including them.

If the agent version is:	You can:
AppManager agent v5.0 (or earlier)	Limit the objects that are discovered by **excluding** particular classes from discovery. If you exclude a particular class, all objects are excluded. You cannot exclude specific instances of objects from within a class.
AppManager agent v5.0.1 (or later)	Limit the objects that are discovered by **including** particular classes in discovery. If you include a particular class, all objects are included. You cannot include specific instances of objects from within a class.

By default, this script is only run once for each computer.

Set the Values tab parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Discovery_ActiveDS job fails. The default is 35.
Discover Active Directory server resources	
Discover objects	Use these parameters to determine which classes of objects are included in discovery and to set depth limits on the number of tree levels to discover. For more information, see Section 2.6.1, “Example of How this Knowledge Script is Used,” on page 20.

Description	How to Set It
Classes to include	Specify the class names you want to discover. Use commas with no spaces to separate more than one class. Enter class names as they appear in the Active Directory schema definition. If you include a particular class, all objects are included. You cannot include specific instances of objects within a class. AppManager does not force discovery of the following classes: ◆ container ◆ organizationalUnit ◆ server ◆ serversContainer ◆ site To discover these classes, you must specifically enter their names in this parameter. Include the organizational Unit class to enable the monitoring of organizational units with the following Knowledge Scripts: ◆ AD_NumberofComputers ◆ AD_NumberofGroups ◆ AD_NumberofObjects ◆ AD_NumberofPrintQueues ◆ AD_NumberofUsers ◆ AD_NumberofUsersLocked Include the server class to discover and use the ReplicationCheckByUSN Knowledge Script. The default is none (no classes specified).

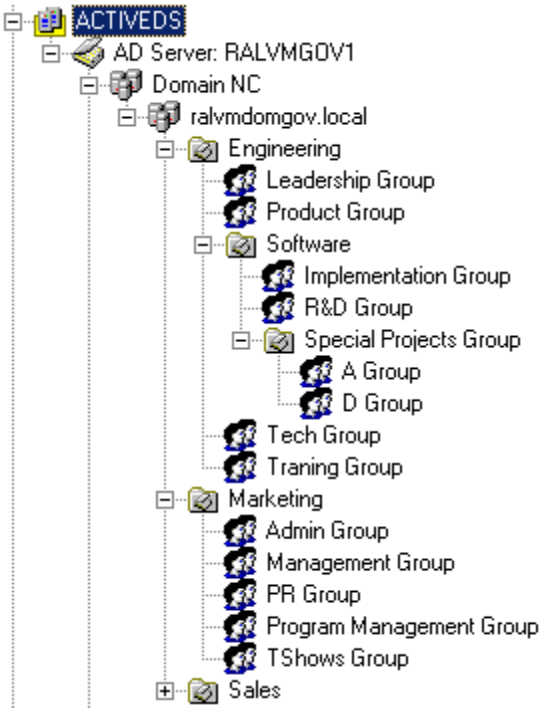
Description	How to Set It
Classes to exclude	Specify the names of classes you do not want to discover. This parameter is applicable only when running this script on an Active Directory server with version 5.0 (or earlier) of the AppManager for Microsoft Active Directory agent. This parameter is not applicable when running this script on an Active Directory server with Version 5.0.1 (or later) of the AppManager for Microsoft Active Directory agent. Discovery information about Active Directory is required to run some Active Directory Knowledge Scripts. Do not exclude the following classes: ◆ container ◆ computer ◆ nTDSDSA ◆ organizationalUnit ◆ server ◆ site ◆ serversContainer Use commas with no spaces to separate the names of multiple classes. Specify class names as they appear in the Active Directory schema definition. The default is `user,group`. **NOTE:** If you exclude a particular class, all objects are excluded. You cannot exclude specific instances of objects from within a class.
Number of children per object	Specify the maximum number of child objects per container level to discover. Keep in mind that a child object can be another container. For more information, see Section 2.6.1, “Example of How this Knowledge Script is Used,” on page 20. Enter 0 to return all child objects for a container. The default is 5 child objects per container.
Number of levels deep to go in tree	Specify the maximum number of container levels deep in the domain object portion of the Active Directory tree to discover. To discover the child objects in a container, specify the level of the child object. For more information, see Section 2.6.1, “Example of How this Knowledge Script is Used,” on page 20. Enter 0 to return the complete tree structure. The default is 5 levels.
Discover domains and trusts?	Select **Yes** to include the Domains and Trusts resource object in the Operator Console TreeView pane. If you enable this parameter, you can use the subsequent parameters to include or exclude types of domains from the Domains and Trusts resource object. The default is Yes.
Include only adjacent domains?	Select **Yes** to limit discovery to domains that have a direct trust relationship to the servers where discovery is performed. By default, discovery is not limited to domains that have a direct trust relationship, and discovery walks transitive trusts within the forest.
Include only domains in forest?	Select **Yes** to limit discovery to domains in the same forest as the servers where discovery is performed. The default is unselected.

Description	How to Set It
Include only Windows 2000 or later trusting domains?	Select **Yes** to limit discovery to Active Directory domains that trust the domain of the server where discovery is performed (incoming trusts). Disable this parameter to include domains regardless of trust direction, including Windows NT domains and non-Windows domains. The default is Yes.
Event Notification	
Raise event if discovery succeeds?	Select **Yes** to raise an event if discovery succeeds. The default is unselected.
Event severity when discovery succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which discovery succeeds. The default is 25.
Raise event if discovery fails?	Select **Yes** to raise an event if discovery fails. The default is Yes.
Event severity when discovery fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which discovery fails. The default is 5.
Raise event if discovery partially succeeds?	Select **Yes** to raise an event if discovery returns some data but also generates warning messages. The default is Yes.
Event severity when discovery partially succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which discovery returns some data but also generates warning messages. The default is 10.
Raise event if discovery is not applicable?	Select **Yes** to raise an event when discovery is not applicable. This type of failure usually occurs when the target computer does not have Active Directory installed or does not have the AppManager for Microsoft Active Directory managed object for Active Directory. The default is Yes.
Event severity when discovery is not applicable	Set the severity level, from 1 to 40, to indicate the importance of an event in which discovery is not applicable. The default is 15.

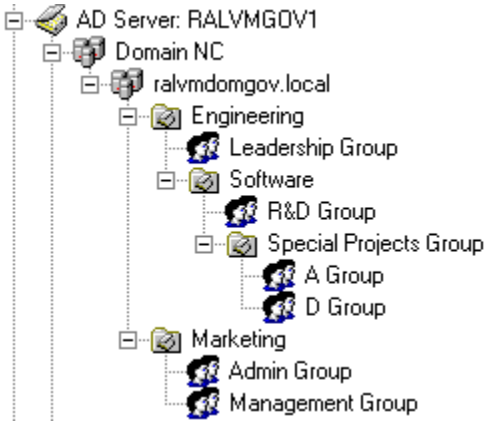
2.6.1 Example of How this Knowledge Script is Used

When you discover Active Directory, the discovered Domain Naming Context and Configuration Container branches can potentially contain millions of objects. This script allows you to control the depth (in container levels) and width (in the number of child objects per container level) of the discovered branches. In addition, you can exclude all objects that belong to a specified class from discovery. By default, this script discovers a minimal number of classes and objects.

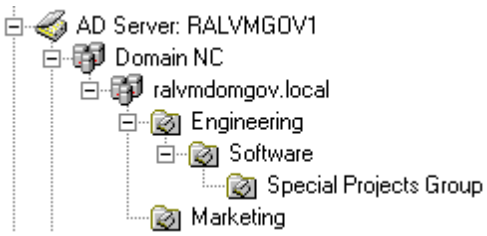
To illustrate how the these discovery parameters work, consider the following example. Assume the complete Domain NC tree has the following structure:



The container-level and children-per-object values are applicable to the containers and objects under `ralvmdomgov.local`. If the number of container levels is 0 (to discover all container levels) and the number of child objects per container level is 2, the discovery result might be similar to the following structure



To further control the number of objects returned, you can exclude particular classes. When you exclude a class, no instances of those objects are displayed. For example, if the "`group`" class is excluded from the discovery, the results of discovery might look something like this.



The specific objects discovered when you use the *Number of children per object* and *Number of levels of the entire tree* parameters depends on how the Active Directory Services Interfaces (ADSI) enumerates the child objects.

2.7 Upgrading Knowledge Script Jobs

If you are using AppManager 8.x or later, the module upgrade process now *retains* any changes you may have made to the parameter settings for the Knowledge Scripts in the previous version of this module. Before AppManager 8.x, the module upgrade process *overwrote* any settings you may have made, changing the settings back to the module defaults.

As a result, if this module includes any changes to the default values for any Knowledge Script parameter, the module upgrade process ignores those changes and retains all parameter values that you updated. Unless you review the management guide or the online Help for that Knowledge Script, you will not know about any changes to default parameter values that came with this release.

You can push the changes for updated scripts to running Knowledge Script jobs in one of the following ways:

- Use the AMAdmin_UpgradeJobs Knowledge Script.
- Use the Properties Propagation feature.

2.7.1 Running AMAdmin_UpgradeJobs

The AMAdmin_UpgradeJobs Knowledge Script can push changes to running Knowledge Script jobs. Your AppManager repository (QDB) must be at version 7.0 or later. In addition, the repository computer must have hotfix 72040 installed, or the most recent AppManager Repository hotfix. To download the hotfix, see the AppManager Suite Hotfixes page.

Upgrading jobs to use the most recent script version allows the jobs to take advantage of the latest script logic while maintaining existing parameter values for the job.

For more information, see the **Help** for the AMAdmin_UpgradeJobs Knowledge Script.

2.7.2 Propagating Knowledge Script Changes

You can propagate script changes to jobs that are running and to Knowledge Script Groups, including recommended Knowledge Script Groups and renamed Knowledge Scripts.

Before propagating script changes, verify that the script parameters are set to your specifications. New parameters may need to be set appropriately for your environment or application.

If you are not using AppManager 8.x or later, customized script parameters may have reverted to default parameters during the installation of the module.

You can choose to propagate only properties (specified in the Schedule and Values tabs), only the script (which is the logic of the Knowledge Script), or both. Unless you know specifically that changes affect only the script logic, you should propagate the properties and the script.

For more information about propagating Knowledge Script changes, see the *Running Monitoring Jobs* chapter of the *Operator Console User Guide for AppManager*.

Propagating Changes to Ad Hoc Jobs

You can propagate the properties and the logic (script) of a Knowledge Script to ad hoc jobs started by that Knowledge Script. Corresponding jobs are stopped and restarted with the Knowledge Script changes.

To propagate changes to ad hoc Knowledge Script jobs:

1. In the Knowledge Script view, select the Knowledge Script for which you want to propagate changes.
2. Right-click the script and select **Properties propagation** > **Ad Hoc Jobs**.
3. Select the components of the Knowledge Script that you want to propagate to associated ad hoc jobs:

Select	To propagate
Script	The logic of the Knowledge Script.
Properties	Values from the Knowledge Script Schedule and Values tabs, such as schedule, monitoring values, actions, and advanced options. If you are using AppManager 8.x or later, the module upgrade process now *retains* any changes you may have made to the parameter settings for the Knowledge Scripts in the previous version of this module.

Propagating Changes to Knowledge Script Groups

You can propagate the properties and logic (script) of a Knowledge Script to corresponding Knowledge Script Group members.

After you propagate script changes to Knowledge Script Group members, you can propagate the updated Knowledge Script Group members to associated running jobs. For more information, see “Propagating Changes to Ad Hoc Jobs” on page 22.

To propagate Knowledge Script changes to Knowledge Script Groups:

1. In the Knowledge Script view, select the Knowledge Script Group for which you want to propagate changes.
2. Right-click the Knowledge Script Group and select **Properties propagation** > **Ad Hoc Jobs**.
3. (Conditional) If you want to exclude a Knowledge Script member from properties propagation, deselect that member from the list in the Properties Propagation dialog box.

4 Select the components of the Knowledge Script that you want to propagate to associated Knowledge Script Groups:

Select	To propagate
Script	The logic of the Knowledge Script.
Properties	Values from the Knowledge Script Schedule and Values tabs, such as schedule, monitoring values, actions, and advanced options. If you are using AppManager 8.x or later, the module upgrade process now *retains* any changes you may have made to the parameter settings for the Knowledge Scripts in the previous version of this module.

5 Click **OK**. Any monitoring jobs started by a Knowledge Script Group member are restarted with the job properties of the Knowledge Script Group member.

3 AD Knowledge Scripts

To help you set up AppManager for Microsoft Active Directory monitoring in accordance with NetIQ recommended best practices guidelines, five Knowledge Script Groups are provided. For more information, see Section 3.48, “AD Knowledge Script Groups,” on page 107.

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**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

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

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

Knowledge Script	What It Does
ReplQueueLen	Monitors the queue length for unprocessed Active Directory replication synchronization requests.
ReplSysVol	Monitors SysVol folder replication.
ResponseTime	Monitors the connection and read response times from the target computer to a specified Active Directory domain controller.
SearchStat	Monitors the number of Active Directory search operations per second.
ServerHealth	Monitors the health of an Active Directory domain controller.
SyncRequest	Monitors Active Directory synchronization requests and the percentage of replication synchronization requests that fail.
WriteStat	Monitors the number of Active Directory write operations per second.
AD Knowledge Script Groups	
AD	Performs essential monitoring for Active Directory domain controllers using job delegation.
AD (all DCs)	Performs essential monitoring for all domain controllers.
AD (one DC per domain)	Performs essential monitoring for a single domain controller in each domain.
AD (one DC per forest)	Performs essential monitoring for a single domain controller in a forest.
AD (one DC per site)	Performs essential monitoring for a single domain controller per site.

3.1 AD Knowledge Script Job Delegation

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

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

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

Use the job delegation feature instead of selecting and re-selecting the DCs for a Knowledge Script job. Instead of re-deploying the script every time a server role changes, you can select a regular schedule and deploy the script once. The script then automatically runs only on the DCs holding a certain server role. You can also avoid creating special server groups to deploy scripts to, say, a DC from every domain. Instead, you can enable job delegation and run the script on all DCs in the forest. The job will run only on DCs holding the server role you selected — one per domain — not on every DC in the forest.

Included as part of the recommended Knowledge Script Groups (KSGs) in AppManager for Active Directory is a KSG named “AD” that uses the job delegation feature. For more information, see Section 3.49, “AD,” on page 108.

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

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

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

The Knowledge Script job delegation feature also allows and event to be raised when a DC assumes the selected server role.

The following scripts offer job delegation:

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

3.2 Authentications

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

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

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

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

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

Performance Objects	Counters
NTDS	Kerberos Authentications
Security System-Wide Statistics	NTLM Authentications
NOTE: The Authentication Knowledge Script gathers values from the Security System-Wide Statistics performance object only when the Domain Controller where it runs is the Windows Server 2008 version or later.	

3.2.1 Resource Object

Active Directory domain controller

3.2.2 Default Schedule

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

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

3.2.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Monitor authentication rate	
Event Notification	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Authentications job fails. The default is 35.
Raise event if Kerberos authentication rate exceeds threshold?	Select Yes to raise an event if the Kerberos authentication rate exceeds the threshold you set. The default is Yes.
Threshold -- Maximum rate of Kerberos authentications	Specify the maximum number of Kerberos authentications per second allowed during any interval before an event is raised. The default is 50 authentications per second.
Event severity when Kerberos authentication rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the Kerberos authentication rate exceeds the threshold. The default is 20.
Raise event if NTLM authentication rate exceeds threshold?	Select Yes to raise an event if the NTLM authentication rate exceeds the threshold you set. The default is Yes.

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

3.3 BridgeheadChange

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

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

3.3.1 Resource Objects

Active Directory domain controller

3.3.2 Default Schedule

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

3.3.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the BridgeheadChange job fails. The default is 35.

Parameter	How to Set It
Monitor bridgehead server changes	
Enable job delegation?	Select Yes to enable the delegation of the job to another server where appropriate. If enabled, the job runs on the computer that holds the server role (Domain Master or Schema Master) that you selected for the *Delegate forest-wide monitoring to the...* parameter. The default is unselected.For more information, see Section 3.1, “AD Knowledge Script Job Delegation,” on page 27.
Delegate forest-wide monitoring to the	Select the server role to delegate the job to: **Domain Master** or **Schema Master**. By default, the job is delegated to the Domain Master.
Raise event when DC assumes this role?	If you enabled job delegation, set to Yes to enable events if the DC assumes the server role you selected for the *Delegate forest-wide monitoring to the...* parameter. The event message indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate forest-wide monitoring to the...* parameter. The default is 30.
Raise event when DC relinquishes this role?	If you enabled job delegation, set to Yes to enable events if the DC gives up the server role you selected for the *Delegate forest-wide monitoring to the...* parameter. The event message indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate forest-wide monitoring to the...* parameter. The default is 30.
Event Notification	
Raise event if changes to bridgehead servers are detected?	Select Yes to raise an event if changes to the bridgehead servers are detected. The default is Yes.
Event severity when changes detected	Set the severity level, from 1 to 40, to indicate the importance of an event in which changes to the bridgehead servers are detected. The default is 25.
Data Collection	
Collect data for changes to bridgehead servers?	Select Yes to collect data for charts and reports. If enabled, data collection returns the number of bridgehead servers for the interval. The default is unselected.

3.4 CacheHitRate

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

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

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

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

Performance Objects	Counter
NTDS	DS Name Cache hit rate
DirectoryServces	

3.4.1 Resource Object

Active Directory domain controller

3.4.2 Default Schedule

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

3.4.3 Setting Parameter Values

The default settings for the **Advanced** tab on the Properties dialog box are overridden for this script. Specifically, the *Collapse duplicates*

option is disabled, and the *Raise event if event condition occurs* option is set to 3 times within 3 job iterations.

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the CacheHitRate job fails. The default is 35.
Monitor cache hit rate	
Event Notification	
Raise event if cache hit rate falls below threshold?	Select Yes to raise an event if the cache hit rate falls below the threshold you set. The default is Yes.
Threshold -- Minimum cache hit rate	Specify the minimum percentage of time that requested data should be found in the cache before an event is raised. The default is 93%.
Event severity when cache hit rate falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the cache hit rate falls below the threshold. The default is 20.
Data Collection	

Parameter	How to Set It
Collect data for cache hit rate?	Select Yes to collect data for charts and reports. If enabled, data collection returns the name cache hit rate for the interval. By default, data is not collected.

3.5 ClientSessions

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

- Lightweight Directory Access Protocol (LDAP) clients
- Address book clients (AB clients)
- Exchange Directory Service clients (XDS clients)

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

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

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

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

Performance Objects	Counters
NTDS	LDAP Client Sessions
DirectoryServices	AB Client Sessions
	XDS Client Sessions

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

```
Number of AB client sessions + Number of LDAP client sessions + Number of XDS
client sessions
```

3.5.1 Resource Objects

Active Directory domain controller

3.5.2 Default Schedule

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

3.5.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ClientSessions job fails. The default is 35.
Monitor number of client sessions	
Event Notification	
Raise event if number of client sessions exceeds threshold?	Select Yes to raise an event if the number of client sessions exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of client sessions	Specify the maximum number of active client sessions allowed during an interval before an event is raised. The default is -1 sessions. You must change the default setting to run this script. You should first collect data to establish a baseline, then specify a threshold appropriate to your environment.
Event severity when client sessions exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of client sessions exceeds the threshold you set. The default is 20.
Data Collection	
Collect data for number of client sessions?	Select Yes to collect data for charts and reports. If enabled, data collection returns the number of client sessions of each type for the interval. The default is unselected.

3.5.4 Example of Using this Knowledge Script

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

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

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

3.6 ConnectivityObject

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

3.6.1 Resource Objects

Any Windows computer

3.6.2 Default Schedule

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

3.6.3 Setting Parameter Values

Set the following parameters as needed:

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

3.7 DatabaseSize

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

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

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

3.7.1 Resource Objects

Active Directory domain controller

3.7.2 Default Schedule

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

3.7.3 Setting Parameter Values

Set the following parameters as needed:

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

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

3.8 DCAdvertised

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

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

3.8.1 Resource Objects

Active Directory domain controller

3.8.2 Default Schedule

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

3.8.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DCAdvertised job fails. The default is 35.
Monitor directory service availability	
Event Notification	
Raise event if directory service is unavailable?	Select Yes to raise an event if the directory service is unavailable. The default is Yes.

Description	How to Set It
Threshold -- Maximum percentage of disk space used	Specify the maximum percentage of logical disk space that can be used by the Active Directory database file before . The default is 80%.
Event severity when directory service is unavailable	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a directory service is unavailable. The default is 10.
Data Collection	
Collect data for directory service availability?	Select Yes to collect data for charts and reports. If enabled, data collection returns: ◆ 100 -- the domain controller is advertising, or ◆ 0 -- the domain controller is not advertising. The default is unselected.

3.9 DCHealthMonitor

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

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

TIP: If you use this script, you should not need to perform additional operating system monitoring for CPU, memory, or disk space usage.

3.9.1 Resource Objects

Active Directory domain controller

3.9.2 Default Schedule

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

3.9.3 Setting Parameter Values

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

Set the following parameters as needed:

Parameter	How to Set It
General Settings	

Parameter	How to Set It
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DCHealthMonitor job fails. The default is 35.
Monitor CPU, memory, and disk utilization?	
Event Notification	
Raise event if CPU utilization exceeds threshold?	Select Yes to raise an event if CPU usage exceeds the threshold you set. The default is Yes.
Threshold -- Maximum CPU utilization	Specify the maximum percentage of CPU resources that can be used by the Active Directory domain controller before an event is raised. The default is 90%.
Event severity when CPU utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold. The default is 5.
Raise event if memory utilization exceeds threshold?	Select Yes to raise an event if memory usage exceeds the threshold you set. The default is Yes.
Threshold -- Maximum memory utilization	Specify the maximum percentage of memory resources that can be used by the Active Directory domain controller before an event is raised. The default is 90%
Event severity when memory utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which memory usage exceeds the threshold. The default is 5.
Raise event if disk utilization exceeds threshold?	Select Yes to raise an event is disk usage exceeds the threshold you set. The default is Yes.
Threshold -- Maximum disk utilization	Specify the maximum percentage of disk space that can be used by the Active Directory domain controller before an event is raised. The default is 90%.
Event severity when disk utilization exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which disk usage exceeds the threshold. The default is 5.
Data Collection	
Collect data for system CPU utilization?	Select Yes to collect data for charts and reports. If enabled, data collection returns the CPU usage of the server as a percentage of total CPU time. The default is unselected. **Tip** Enable this parameter for domain controller load trend analysis.
Collect data for system memory utilization?	Select Yes to collect data for charts and reports. If enabled, data collection returns the memory usage of the server (as a percentage of total system memory). The default is unselected. **Tip** Enable this parameter for domain controller load trend analysis.
Collect data for disk utilization?	Select Yes to collect data for charts and reports. If enabled, data collection returns the disk usage of the server (as a percentage of total disk space). The default is unselected. **Tip** Enable this parameter for domain controller load trend analysis.

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

3.10 DCInSiteConnectivity

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

3.10.1 Resource Objects

Active Directory site container on a domain controller

3.10.2 Default Schedule

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

3.10.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DCInSiteConnectivity job fails. The default is 35.
Monitor connectivity to DCs in the same site	
Enable job delegation?	Select Yes to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the Inter-Site Topology Generator (ISTG) server role. The default is unselected. For more information, see Section 3.1, “AD Knowledge Script Job Delegation,” on page 27.
Delegate site-wide monitoring to the	Indicates the server role to which the job should be delegated, the ISTG.
Raise event when DC assumes this role?	If you enabled job delegation, set to Yes to raise an event if the domain controller (DC) assumes the ISTG server role. The event indicates that the monitored computer has assumed that role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the ISTG server role. The default is 30.
Raise event when DC relinquishes this role?	If you enabled job delegation, set to Yes to raise an event if the DC gives up the ISTG server role. The event indicates that the monitored computer has relinquished that role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the ISTG server role. The default is 30.
Event Notification	
Raise event when connectivity to domain controller fails?	Select Yes to raise an event if connectivity to the DC fails. The default is Yes.
Event severity when domain controller down	Set the severity level, from 1 to 40, to indicate the importance of an event in which connectivity to the DC fails. The default is 5.
Data Collection	
Collect data for site connectivity percentage?	Select Yes to collect data for charts and reports. If enabled, data collection returns the connectivity percentage for the site. For example, if 9 of the 10 domain controllers in the site are accessible, connectivity is 90%. The default is unselected.

3.11 DomainConnectivity

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

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

The most common reason for broken trust relationships are:

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

3.11.1 Resource Objects

Active Directory trusted domain

3.11.2 Default Schedule

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

3.11.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DomainConnectivity job fails. The default is 35.
Monitor connectivity to selected domains	
Enable job delegation?	Select Yes to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role that you selected for the *Delegate forest-wide monitoring to the...* parameter. The default is unselected. For more information, see Section 3.1, “AD Knowledge Script Job Delegation,” on page 27.
Delegate domain-wide monitoring to the	Select the server role to which the job should be delegated: **Primary Domain Controller (PDC)**, **Infrastructure Master**, or **RID Master**. The default is PDC.
Raise event when DC assumes this role?	If you enabled job delegation, set to Yes to raise an event if the DC assumes the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30.

Parameter	How to Set It
Raise event when DC relinquishes this role?	If you enabled job delegation, set to Yes to raise an event if the DC gives up the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30.
Event Notification	
Raise event when domain connectivity fails?	Select **Yes** to raise an event if connectivity to a domain fails. The default is Yes.
Event severity when domain connectivity fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which connectivity to a domain fails. The default is 10.
Data Collection	
Collect data for connection status?	Select Yes to collect data for charts and reports. If enabled, data collection returns: ◆ 100 -- the connection to a trusted domain was successful, or ◆ 0 -- the connection failed. The default is unselected.

3.12 EnumerateSites

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

3.12.1 Resource Objects

Active Directory domain controller

3.12.2 Default Schedule

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

3.12.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the EnumerateSites job fails. The default is 35.

Parameter	How to Set It
Monitor the number of sites in forest	
Enable job delegation?	Select Yes to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role (Domain Master or Schema Master) that you selected for the *Delegate forest-wide monitoring to the...* parameter (see below). The default is unselected. For more information, see Section 3.1, “AD Knowledge Script Job Delegation,” on page 27.
Delegate forest-wide monitoring to the	Select the server role to which the job should be delegated: **Domain Master** or **Schema Master**. The default is Domain Master.
Raise event when DC assumes this role?	If you enabled job delegation, set to Yes to raise an event if the DC assumes the server role you selected for the *Delegate forest-wide monitoring to the...* parameter. The event message indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate forest-wide monitoring to the...* parameter. The default is 30.
Raise event when DC relinquishes this role?	If you enabled job delegation, set to Yes to raise an event if the DC gives up the server role you selected for the *Delegate forest-wide monitoring to the...* parameter. The event message indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate forest-wide monitoring to the...* parameter. The default is 30.
Event Notification	
Raise event when changes to sites occur?	Select Yes to raise an event if changes occur to sites in the forest. The default is Yes.
Event severity when number of sites changes	Set the severity level, from 1 to 40, to indicate the importance of an event in which changes occur to sites in the forest. The default is 25.
Data Collection	
Collect data for number of sites in forest?	Select Yes to collect data for charts and reports. If enabled, data collection returns the number of sites. The default is unselected.

3.13 EventLog

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

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

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

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

NOTE

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

3.13.1 Resource Object

Active Directory domain controller

3.13.2 Default Schedule

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

3.13.3 Setting Parameter Values

Set the following parameters as needed:

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

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

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

3.14 EventLog (NetLogon)

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

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

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

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

NOTE: Only the most recent batch of events can be viewed in the data point detail message. For example, assume you set this script to scan all previous entries in the event log and list ten matching entries in each event detail message. When the script runs, 30 entries are found that match your filtering criteria. In this case, the script would create three child events for the interval.

Each child event would have ten entries: the oldest matching entries in one child event batch, the second oldest in a second batch, and the most recent in a third batch.

If this same job is collecting data and you view the detail message for the interval, only the entries from the third child event (Batch 3) are displayed.

3.14.1 Resource Objects

Active Directory domain controller

3.14.2 Default Schedule

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

3.14.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the EventLog (NetLogon) job fails. The default is 35.
Monitor Windows System log for NetLogon events	
Start with events in past	Set this parameter to control checking for the first job iteration. After the first iteration, checking of the log is incremental: ◆ **-1**--all the existing log entries ◆ **n**--entries from the past *n* hours (8 for the past 8 hours, 50 for the past 50 hours, etc.) ◆ **0**--no previous entries (only search from the present moment forward) The default is 0.
Filtering	
Event Types	
Error	Select Yes to monitor Error entries. The default is Yes.
Warning	Select Yes to monitor Warning entries. The default is Yes.
Information	Select Yes to monitor Information Entries. The default is unselected.
Other	
Filter -- Source	To monitor events generated by a particular source, enter an appropriate search string. This script looks for matching entries in the Event Log's **Source** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter -- Category	To monitor events in a particular category, such as Server or Logon, enter an appropriate search string. This script looks for matching entries in the Event Log's **Category** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.

Description	How to Set It
Filter -- Event ID	To monitor particular event IDs, enter an appropriate search string or ID range, for example, 100-2000. This script looks for matching entries in the Event Log's **Event** field. Multiple IDs and ranges can be entered, separated by commas and no spaces. For example: `1,2,10-15,202`. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter -- User	To monitor events associated with a particular user, enter an appropriate search string, for example, `<domain name>\<user name>`. This script looks for matching entries in the Event Log's **User** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter -- Computer	To monitor events generated by a particular computer, enter an appropriate search string. This script looks for matching entries in the Event Log's **Computer** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Filter -- Description	To monitor events with a particular detail description or containing keywords in the description, enter an appropriate search string. This script looks for matching entries in the Event Log's **Description** field. Multiple strings can be entered separated by commas. The search string can contain criteria used to include entries, exclude entries, or both. Separate the include and exclude criteria with a colon (:). If you are specifying only include criteria, the colon is not necessary.
Event Notification	
Raise event if new log entries found?	Select Yes to raise an event if new log entries are found. The default is Yes.
Maximum number of entries per event message	Specify the maximum number of entries to be recorded into each event's detail message. If this script finds more entries from the log than can be put into one event message, it will return multiple events to report all of the outstanding entries in the log. The default is 1 entry.
Event severity when new event log entries found	Set the severity level, from 1 to 40, to indicate the importance of an event in which new log entries are fund. The default is 10.
Data Collection	
Collect data for number of matching entries?	Select Yes to collect data for charts and reports. If enabled, data collection returns the number of Event Log entries that match your filtering criteria. Additional information is supplied in the data detail message. The default is unselected.

3.15 EventLog (W32Time)

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

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

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

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

NOTE: Only the most recent batch of events can be viewed in the data point detail message. For example, assume you set this script to scan all previous entries in the event log and list ten matching entries in each event detail message.

When the script runs, 30 entries are found that match your filtering criteria. In this case, the script would create three child events for the interval. Each child event would have ten entries: the oldest matching entries in one child event batch, the second oldest in a second batch, and the most recent in a third batch.

If this same job is collecting data and you view the detail message for the interval, only the entries from the third child event (Batch 3) are displayed.

3.15.1 Resource Objects

Active Directory domain controller

3.15.2 Default Schedule

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

3.15.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the EventLog (W32Time) job fails. The default is 35.
Monitor Windows System log for time synchronization events	

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

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

3.16 FSMOChange

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

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

3.16.1 Resource Objects

Active Directory domain

3.16.2 Default Schedule

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

3.16.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the FSMOChange job fails. The default is 35.
Monitor changes to FSMO roles	
Enable job delegation?	Select Yes to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role that you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is unselected. For more information, see Section 3.1, “AD Knowledge Script Job Delegation,” on page 27.
Delegate domain-wide monitoring to the	Select the server role to which the job should be delegated: **Primary Domain Controller (PDC)**, **Infrastructure Master**, or **RID Master**. The default is PDC.
Raise event when DC assumes this role?	If you enabled job delegation, set to Yes to raise events if the DC assumes the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30.
Raise event when DC relinquishes this role?	If you enabled job delegation, set to Yes to raise events if the DC gives up the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30.
Event Notification	
Raise event if change to FSMO roles detected?	Select Yes to raise an event if changes to FSMO roles are detected. The default is Yes.
Event severity when change detected	Set the severity level, from 1 to 40, to indicate the importance of an event in which changes to FSMO roles are detected. The default severity level is 20.
Data Collection	
Collect data for changes to FSMO roles?	Select Yes to collect data for charts and reports. If enabled, data collection returns: ◆ 100 -- no change to the FSMO roles detected, or ◆ 0 -- change to FSMO role detected. The default is unselected.

3.17 FSMOHealth

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

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

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

3.17.1 Job Delegation and the FSMOHealth Knowledge Script

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

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

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

3.17.2 Deploying this Script Without Job Delegation

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

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

3.17.3 Resource Objects

Active Directory domain

3.17.4 Default Schedule

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

3.17.5 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the FSMOHealth job fails. The default is 35.
Monitor connectivity to FSMO role holders	
Enable job delegation?	Select Yes to enable the delegation of the job to another server where appropriate. If enabled, the runs job on each DC that holds a domain FSMO role. The default is unselected. For more information, see Section 3.1, "AD Knowledge Script Job Delegation," on page 27.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC assumes a domain FSMO role. The event indicates that the monitored computer has assumed a domain FSMO role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes a domain FSMO role. The default is 30.
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up a domain FSMO role. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes a domain FSMO role. The default is 30.
Event Notification	
Raise event if domain controller inaccessible?	Select Yes to raise an event if a DC that holds a FSMO role is inaccessible. The default is Yes.
Event severity when domain controller inaccessible	Set the severity level, from 1 to 40, to indicate the importance of an event in which a DC that holds a FSMO role is inaccessible. The default is 10.
Data Collection	
Collect data for inaccessible DC and its role?	Select Yes to collect data for charts and reports. If enabled, data collection returns a value of 100 if there is no change to the FMSO roles, or a value of 0 if there has been a change during the interval. The default is unselected.

3.18 FSMOPlacement

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

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

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

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

3.18.1 Resource Objects

Active Directory domain

3.18.2 Default Schedule

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

3.18.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the FSMOPlacement job fails. The default is 35.
Monitor FSMO role placement	
Enable job delegation?	Select Yes to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role that you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is unselected. For more information, see Section 3.1, "AD Knowledge Script Job Delegation," on page 27.
Delegate domain-wide monitoring to the	Select the server role to which the job should be delegated: **Primary Domain Controller (PDC)**, **Infrastructure Master**, or **RID Master**. The default is PDC.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC assumes the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30.
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30.
Event Notification	
Raise event if role placement invalid?	Select Yes to raise an event if the FSMO role placement is invalid. The default is Yes.
Event severity when role placement invalid	Set the severity level, from 1 to 40, to indicate the importance of an event in which the FSMO role placement is invalid. The default is 10.

Parameter	How to Set It
Data Collection	
Collect data for role placement status (valid or invalid)?	Select Yes to collect data for charts and reports. If enabled, data collection returns: ◆ 100 -- the FMSO role placement is valid, or ◆ 0 -- a problem with role placement was found. The default is unselected.

3.19 GlobalCatalogChange

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

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

3.19.1 Resource Objects

Active Directory domain controller

3.19.2 Default Schedule

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

3.19.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the GlobalCatalogChange job fails. The default is 35.
Monitor global catalog server changes	
Enable job delegation?	Select Yes to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role (Domain Master or Schema Master) that you selected for the *Delegate forest-wide monitoring to the...* parameter. The default is unselected. For more information, see Section 3.1, “AD Knowledge Script Job Delegation,” on page 27.
Delegate forest-wide monitoring to the	Select the server role to which the job should be delegated: **Domain Master** or **Schema Master**. The default is Domain Master.

Parameter	How to Set It
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC assumes the server role you selected for the *Delegate forest-wide monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate forest-wide monitoring to the...* parameter. The default is 30.
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up the server role you selected for the *Delegate forest-wide monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate forest-wide monitoring to the...* parameter. The default is 30.
Event Notification	
Raise event if global catalog server changes detected?	Select Yes to raise an event if GC servers are added or run. The default is Yes.
Event severity when changes detected	Set the severity level, from 1 to 40, to indicate the importance of an event in which GC servers are added or run. The default is 25.
Data Collection	
Collect data for global catalog server changes?	Select Yes to collect data for charts and reports. If enabled, data collection returns: ◆ 0 -- no changes to the list of global catalog servers, or ◆ 1 -- there have been changes to the list of global catalog servers. The default is unselected.

3.20 GlobalCatalogHealth

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

3.20.1 Resource Objects

Active Directory domain controller

3.20.2 Default Schedule

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

3.20.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the GlobalCatalogHealth job fails. The default is 35.
Monitor connectivity to global catalog servers	
Scope of global catalog monitoring	Select **site(s)** or **forest** to indicate the scope within which you want to monitor your global catalog servers.
Site list (comma-separated, no spaces)	Specify a list of sites to monitor. Separate names by commas and no spaces. The list can contain no more than 4096 characters.
Full path to file with list of sites	You can use a text file that contains a list of sites, rather than using the previous parameter. Specify the path to that file here. The path can be to a file on the computer where the AppManager agent is installed (for example, `C:\AMAgent\sitelist`), or a UNC path if the file exists on a different computer (for example, `\\Server1\SiteLists\sitelist`). The file should contain one site per line. The AppManager agent must have read permission for the file.
Enable job delegation?	Select Yes to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the Inter-Site Topology Generator (ISTG) server role. The default is unselected. For more information, see Section 3.1, “AD Knowledge Script Job Delegation,” on page 27.
Delegate site-wide monitoring to the	Indicates the server role to which the job should be delegated, the ISTG.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the domain controller (DC) assumes the ISTG server role. The event indicates that the monitored computer has assumed that role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the ISTG server role. The default is 30.
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up the ISTG server role. The event indicates that the monitored computer has relinquished that role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the ISTG server role. The default is 30.
Event Notification	
Raise event if connection to global catalog fails?	Select Yes to raise an event if the connection to the GC fails. The default is Yes.
Event severity when connection fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the connection to the GC fails. The default is 10.
Data Collection	

Parameter	How to Set It
Collect data for global catalog status?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns: ◆ Percentage of Global Catalog Servers Up % ◆ Number of Global Catalog Servers Up GCs ◆ Number of Global Catalog Servers Down GCs

3.21 InboundReplStat

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

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

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

3.21.1 Resource Objects

Active Directory domain controller

3.21.2 Default Schedule

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

3.21.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the InboundReplStat job fails. The default is 35.
Monitor inbound replication rate	

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

3.22 InterReplTraffic

Use this Knowledge Script to monitor the replication traffic from the DRA (Directory Replication Agent) between Active Directory sites, sometimes referred to as inter-site replication traffic. This script raises an event if either the inbound bytes per second or the outbound bytes per second exceeds the threshold for the specified consecutive number of monitoring intervals.

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

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

3.22.1 Resource Objects

Active Directory domain controller

3.22.2 Default Schedule

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

3.22.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the InterReplTraffic job fails. The default is 35.
Monitor intersite replication traffic	
Event Notification	
Raise event when threshold exceeded too often?	Select **Yes** to raise an event if the replication traffic threshold is exceeded too often. The default is Yes.
Threshold -- Maximum inbound or outbound bytes per second	Specify the maximum number of inbound or outbound replication bytes allowed per second before an event is raised. The default is 60000 bytes per second. Inbound bytes and outbound bytes per second are monitored separately and checked against this threshold. This script raises an event if either the inbound rate or the outbound rate exceeds this threshold more than *n* times.
Maximum consecutive intervals threshold can be exceeded	Specify the maximum number of consecutive intervals the inbound or outbound rate can be exceeded before raising an event. The default is 1 interval. Because replication traffic can have periodic spikes, consider setting this parameter to a higher value to filter out unnecessary events. For example, you can allow the inbound/outbound byte rate to exceed the threshold 3 to 4 times before an event is raised.
Event severity when replication traffic exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which replication traffic exceeds the threshold more than *n* times. The default is 20.
Data Collection	
Collect data for inbound and outbound bytes per second?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of inbound bytes per second and the number of outbound bytes per second. The default is unselected.

3.23 IntraReplTraffic

Use this Knowledge Script to monitor the replication traffic from the DRA (Directory Replication Agent) within an Active Directory site (intrasite replication traffic). You specify the maximum number of inbound or outbound bytes per second and the number of consecutive times the threshold can be

exceeded before raising an event. This script raises an event if the rate of either inbound bytes per second or outbound bytes per second exceeds the threshold for the specified consecutive number of monitoring intervals.

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

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

3.23.1 Resource Objects

Active Directory domain controller

3.23.2 Default Schedule

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

3.23.3 Setting Parameter Values

Set the following parameters as needed:

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

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

3.24 KCCConnections

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

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

3.24.1 Resource Objects

Active Directory domain controller

3.24.2 Default Schedule

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

3.24.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the KCCConnections job fails. The default is 35.
Monitor number of KCC connections	

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

3.25 KCCDisabled

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

NOTE: Enabling the KCC requires Domain Admin permission. If you want to use this Knowledge Script to enable the KCC, set the AppManager agent to run as an account with Domain Admin permission, or specify an account and password with Domain Admin permission.

3.25.1 Resource Object

Active Directory domain controller

3.25.2 Default Schedule

The default interval for this script is Every hour.

3.25.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	

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 KCCDisabled job fails. The default is 35.
Monitor KCC status	
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the Inter-Site Topology Generator (ISTG) server role. The default is unselected. For more information, see Section 3.1, “AD Knowledge Script Job Delegation,” on page 27.
Delegate site-wide monitoring to the	Indicates the server role to which the job should be delegated, the ISTG.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the domain controller (DC) assumes the ISTG server role. The event indicates that the monitored computer has assumed that role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the ISTG server role. The default is 30.
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up the ISTG server role. The event indicates that the monitored computer has relinquished that role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the ISTG server role. The default is 30.
Event Notification	
Raise event if KCC is disabled?	Select **Yes** to raise an event if the KCC is disabled. The default is Yes.
Event severity when KCC is disabled	Set the severity level, from 1 to 40, to indicate the importance of an event in which the KCC is disabled. The default is 20.
Raise event if KCC is enabled?	Select **Yes** to raise an event if the KCC is enabled. The default is unselected.
Event severity when KCC is enabled	Set the severity level, from 1 to 40, to indicate the importance of an event in which the KCC is enabled. The default is 25.
Data Collection	
Collect data for KCC status?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns: ◆ 100 -- KCC is enabled ◆ 0 -- KCC is disabled. The default is unselected.
Remediation	
Enable KCC for intrasite topology generation?	Select **Yes** to reenable the KCC for intrasite topology generation if the KCC is disabled. The default is Yes.
Enable KCC for intersite topology generation?	Select **Yes** to reenable the KCC for intersite topology generation if the KCC is disabled. The default is unselected.
Account to use to enable KCC (leave blank to use the MC account)	Specify the account to be used by AppManager for Microsoft Active Directory to reenable the KCC. Use the format `domain\user` or `user@domain`. Leave this value blank to use the managed client account.

Parameter	How to Set It
Password for this account	Specify the password associated with the account you noted above. The maximum length allowed for the password is 32 characters.

3.26 KDCRequests

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

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

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

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

3.26.1 Resource Objects

Active Directory domain controller

3.26.2 Default Schedule

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

3.26.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the KDCRequests job fails. The default is 35.
Monitor KDC request rate	
Event Notification	
Raise event if KDC request rate exceeds a threshold?	Select **Yes** to raise an event if the KDC request rate exceeds the threshold you set. The default is Yes.

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

3.27 NumberOfComputers

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

3.27.1 Resource Objects

Active Directory domain or organizational unit (OU).

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

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

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

3.27.2 Default Schedule

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

3.27.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance an event in which the NumberOfComputers job fails. The default is 35.
Monitor number of computers	

Parameter	How to Set It
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role that you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is unselected. For more information, see Section 3.1, “AD Knowledge Script Job Delegation,” on page 27.
Delegate domain-wide monitoring to the	Select the server role to which the job should be delegated: **Primary Domain Controller (PDC)**, **Infrastructure Master**, or **RID Master**. The default is PDC.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC assumes the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30.
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30.
Event Notification	
Raise event if number of computers exceeds threshold?	Select **Yes** to raise an event if the number of computers in the domain or OU exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of computers	Specify the maximum number of computers that can be in the domain or OU before an event is raised. The default is -1 computer. **NOTE:** You must change the default setting to run this script. Collect data to establish a baseline, then specify a threshold appropriate for your environment.
Event severity when number of computers exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of computers exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of computers?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of computers detected during the monitoring interval. The default is unselected.
Number of computers to return when collecting data (0 for all computers)	Specify the number of computers you want returned when collecting data. For example, if you set this parameter to 500 and the domain contains 2,000 computers, only the first 500 computers are returned in the event message. Select 0 to return all computers. The default is 500 computers.

3.28 NumberOfDCs

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

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

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

3.28.1 Resource Objects

Active Directory domain controller

3.28.2 Default Schedule

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

3.28.3 Setting Parameter Values

Set the following parameters as needed:

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

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

Parameter	How to Set It
Full path to file with list of domains or sites	To instruct this script to read from a file with a list of domains or sites, rather than entering a list in the *List of fully qualified domains or sites to monitor* parameter, enter the full directory path to that file here. The path can be to a file on the computer where the AppManager agent is installed (for example, `C:\AMAgent\domainsitelist`), or a UNC path if the file exists on a different computer (for example, `\\Server1\SiteLists\domainsitelist`). The file should contain one site per line. The AppManager agent must have read permission for the file.
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role that you selected for the *Delegate [scope] monitoring to the...* parameter. The default is unselected. For more information, see Section 3.1, “AD Knowledge Script Job Delegation,” on page 27.
Delegate domain-wide monitoring to the	Select the server role to which the job should be delegated: **Primary Domain Controller (PDC)**, **Infrastructure Master**, or **RID Master**. The default is PDC.
Delegate site-wide monitoring to the	Indicates the server role to which the job should be delegated, the ISTG.
Delegate forest-wide monitoring to the	Select the server role to which the job should be delegated: **Domain Master** or **Schema Master**. The default is Domain Master.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC assumes the server role you selected for the *Delegate [scope] monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate [scope] monitoring to the...* parameter. The default is 30.
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to enable events if the DC gives up the server role you selected for the *Delegate [scope] monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate [scope] monitoring to the...* parameter. The default is 30.
Event Notification	
Raise event if threshold exceeded or not met?	Select **Yes** to raise an event if the number of DCs exceeds or falls below the threshold you set. The default is Yes.
Threshold -- Minimum number of domain controllers	Specify the minimum number of DCs that must exist to prevent an event from being raised. The default is 2 DCs.
Threshold -- Maximum number of domain controllers	Specify the maximum number of DCs that can exist before an event is raised. The default is 20 DCs.
Event severity when threshold exceeded or not met	Set the severity level, from 1 to 40, to indicate the importance of ant in which the number of DCs exceeds or falls below the threshold. The default is 5.

Parameter	How to Set It
Data Collection	
Collect data for number of DCs?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of DCs detected during the monitoring interval. The default is unselected.

3.29 NumberOfGCs

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

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

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

3.29.1 Resource Objects

Active Directory domain controller

3.29.2 Default Schedule

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

3.29.3 Setting Parameter Values

Set the following parameters as needed:

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

Parameter	How to Set It

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

Full path to file with list of domains or sites	To instruct this script to read from a file with a list of domains or sites, rather than entering a list for the *List of fully qualified domains or sites to monitor* parameter, enter the full directory path to that file here. The path can be to a file on the computer where the AppManager agent is installed (for example, `C:\AMAgent\domainsitelist`), or a UNC path if the file exists on a different computer (for example, `\\Server1\SiteLists\domainsitelist`). The file should contain one site per line. The AppManager agent must have read permission for the file.
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role that you selected for the *Delegate [scope] monitoring to the...* parameter. The default is unselected. For more information, see Section 3.1, “AD Knowledge Script Job Delegation,” on page 27.
Delegate domain-wide monitoring to the	Select the server role to which the job should be delegated: **Primary Domain Controller (PDC)**, **Infrastructure Master**, or **RID Master**. The default is PDC.
Delegate site-wide monitoring to the	Indicates the server role to which the job should be delegated, the ISTG.
Delegate forest-wide monitoring to the	Select the server role to which the job should be delegated: **Domain Master** or **Schema Master**. The default is Domain Master.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC assumes the server role you selected for the *Delegate [scope] monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate [scope] monitoring to the...* parameter. The default is 30.
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up the server role you selected for the *Delegate [scope] monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate [scope] monitoring to the...* parameter. The default is 30.
Event Notification	
Raise event if threshold exceeded or not met?	Select **Yes** to raise an event if the number of GC servers exceeds or falls below the threshold you sent. The default is Yes.

Parameter	How to Set It
Threshold -- Minimum number of global catalog servers	Specify the minimum number of GC servers that must exist to prevent an event from being raised. The default is 1 global catalog server.
Threshold -- Maximum number of global catalog servers	Specify the maximum number of GC servers that can exist before an event is raised. The default value is 20 global catalog servers.
Event severity when threshold exceeded or not met	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of GC servers exceeds or falls below the threshold. The default is 20.
Data Collection	
Collect data for number of global catalog server?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of GC servers detected in the interval. The first time the job runs, it also returns a list of all the GC servers. The default is unselected.

3.30 NumberOfGroups

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

3.30.1 Resource Objects

Active Directory domain or organizational unit (OU)

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

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

When you run this script on a domain, the domain and all child OUs will show a job is running. However, when the script is run on a domain, the script runs only on the domain and not on the child OUs.

3.30.2 Default Schedule

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

3.30.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the NumberOfGroups job fails. The default is 35.

Parameter	How to Set It
Monitor number of groups	
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role that you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is unselected. For more information, see Section 3.1, “AD Knowledge Script Job Delegation,” on page 27.
Delegate domain-wide monitoring to the	Select the server role to which the job should be delegated: **Primary Domain Controller (PDC)**, **Infrastructure Master**, or **RID Master**. The default is PDC.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC assumes the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30.
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30.
Event Notification	
Raise event if number of groups exceeds threshold?	Select **Yes** to raise an event if the number of groups exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of groups	Specify the maximum number of groups that can be in the domain, site, or forest before an event is raised. The default is -1 group. **NOTE:** You must change the default setting to run this script. Collect data to establish a baseline, then specify a threshold appropriate to your environment.
Event severity when number of groups exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of groups exceeds the threshold. The default is 20.
Data Collection	
Collect data for number of groups?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of groups detected during the monitoring interval. the default is unselected.
Number of groups to return when collecting data (0 for all groups)	Specify the number of groups you want returned when collecting data. For example, if you set this parameter to 400 and the domain contains 700 groups, only the first 400 groups are returned. Enter 0 to return all groups. The default is 400 groups.

3.31 NumberOfObjects

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

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

TIP: The recommended value for the Threshold -- Maximum number of objects parameter is the current number of objects, plus 10% of that value.

3.31.1 Resource Objects

Active Directory domain or organizational unit (OU)

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

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

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

3.31.2 Default Schedule

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

3.31.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the NumberOfObjects job fails. The default is 35.
Monitor number of objects	
Object class to check (* for all objects)	Select the type of Active Directory object to check: **domain**, **computer**, or **user**. Select an asterisk (*) to check for all objects. The default is none.
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role that you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is unselected. For more information, see Section 3.1, “AD Knowledge Script Job Delegation,” on page 27.
Delegate domain-wide monitoring to the	Select the server role to which the job should be delegated: **Primary Domain Controller (PDC)**, **Infrastructure Master**, or **RID Master**. The default is PDC.

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

3.32 NumberOfPrintQueues

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

3.32.1 Resource Objects

Active Directory domain or organizational unit (OU)

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

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

When you run this script on a domain, the domain and all child OUs will show a job is running. However, when the script is run on a domain, the script runs only on the domain and not on the child OUs.

3.32.2 Default Schedule

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

3.32.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the NumberOfPrintQueues job fails. The default is 35.
Monitor number of print queues	
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role that you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is unselected. For more information, see Section 3.1, “AD Knowledge Script Job Delegation,” on page 27.
Delegate domain-wide monitoring to the	Select the server role to which the job should be delegated: **Primary Domain Controller (PDC)**, **Infrastructure Master**, or **RID Master**. The default is PDC.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC assumes the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30.
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30.
Event Notification	
Raise event if number of printer queues exceeds threshold?	Select **Yes** to raise an event if the number of printer queues exceeds the threshold you set. The default is Yes.

Parameter	How to Set It
Threshold -- Maximum number of printer queues	Specify the maximum number of printer queues that can be in the domain or OU before an event is raised. The default is -1 printer queue. **NOTE:** Change the default setting to run this script. Collect data to establish a baseline, then specify a threshold appropriate to your environment.
Event severity when number of printer queues exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of printer queues exceeds the threshold. The default is 20.
Data Collection	
Collect data for number of printer queues?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of printer queues detected during the monitoring interval. The default is unselected.
Number of printer queues to return when collecting data	Specify the number of printer queues you want returned when collecting data. For example, if you set this parameter to 500 and the domain contains 800 printer queues, only the first 500 printer queues are returned. Enter 0 to return all printer queues. The default is 500 printer queues.

3.33 NumberOfUsers

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

3.33.1 Resource Objects

Active Directory domain or organizational unit (OU).

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

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

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

3.33.2 Default Schedule

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

3.33.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	

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 NumberOfUsers job fails. The default is 35.
Monitor number of users	
Include contacts?	Select **Yes** to include contact objects in your count of the Number of Users. By default this script refers to security users only.
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role that you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is unselected. For more information, see Section 3.1, “AD Knowledge Script Job Delegation,” on page 27.
Delegate domain-wide monitoring to the	Select the server role to which the job should be delegated: **Primary Domain Controller (PDC)**, **Infrastructure Master**, or **RID Master**. The default is PDC.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC assumes the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30.
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30.
Event Notification	
Raise event when number of users exceeds threshold?	Select **Yes** to raise an event if the number of users in an organization unit or domain exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of users	Specify the maximum number of users that can be in the domain or organizational unit before an event is raised. The default is -1 user. **NOTE:** Change the default setting to run this script. Collect data to establish a baseline, then specify a threshold appropriate to your environment.
Event severity when number of users exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of users in the domain or organizational unit exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of users?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of users detected in the interval. The default is unselected.
Number of users to return when collecting data (0 for all users)	Specify the number of users you want returned when collecting data. For example, if you set this parameter to 1000 and the domain or OU contains 10,000 users, only the first 1000 users are returned. Enter 0 to return all users. The default is 1000 users.

3.34 NumberOfUsersLocked

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

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

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

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

3.34.1 Resource Objects

Active Directory domain or organizational unit (OU)

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

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

When you run this script on a domain, the domain and all child OUs will show a job is running. However, when the script is run on a domain, the script runs only on the domain and not on the child OUs.

3.34.2 Default Schedule

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

3.34.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the NumberOfUsersLocked job fails. The default is 35.
Monitor number of locked user accounts	
Omit disabled accounts?	Select **Yes** to ignore disabled user accounts when checking for locked user accounts. By default, this script includes disabled accounts when checking for locked user

Parameter	How to Set It
Enable job delegation?	Select **Yes** to enable the delegation of the job to another server where appropriate. If enabled, runs the job on the selected computer that holds the server role that you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is unselected. For more information, see Section 3.1, “AD Knowledge Script Job Delegation,” on page 27.
Delegate domain-wide monitoring to the	Select the server role to which the job should be delegated: **Primary Domain Controller (PDC)**, **Infrastructure Master**, or **RID Master**. The default is PDC.
Raise event when DC assumes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC assumes the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has assumed the selected role. The default is Yes.
Event severity when DC assumes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC assumes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30.
Raise event when DC relinquishes this role?	If you enabled job delegation, set to **Yes** to raise events if the DC gives up the server role you selected for the *Delegate domain-wide monitoring to the...* parameter. The event indicates that the monitored computer has relinquished the selected role. The default is Yes.
Event severity when DC relinquishes this role	Set the severity level, from 1 to 40, to indicate the importance of an event in which the DC relinquishes the role you selected for the *Delegate domain-wide monitoring to the...* parameter. The default is 30.
Event Notification	
Raise event if number of locked user accounts exceeds threshold?	Select **Yes** to raise an event if the number of locked user accounts exceeds the threshold you set. The default is Yes.
Threshold -- Maximum number of locked user accounts	Specify the maximum number of locked user accounts that can be in the domain naming context before an event is raised. The default is 10 locked accounts.
Event severity when number of locked accounts exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of locked user accounts exceeds the threshold. The default is 5.
Data Collection	
Collect data for number of locked user accounts?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of locked user accounts detected in the interval. The default is unselected.
Remediation	
Unlock accounts that are locked?	Select **Yes** to automatically unlock locked user accounts. The default is unselected.
List of accounts to unlock	If you enabled the previous parameter, list specific user accounts to unlock, or leave the field blank to unlock all locked user accounts. Separate multiple entries with commas and no spaces. For example, to only unlock specific accounts, enter: `wolfpack,serge,elan` **NOTE:** Use the account name as it is displayed in the Users and Computers administrative tool. The names specified will match any part of an account name.

3.35 OutboundReplStat

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

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

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

3.35.1 Resource Objects

Active Directory domain controller

3.35.2 Default Schedule

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

3.35.3 Setting Parameter Values

Set the following parameters as needed:

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

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

3.36 PropertyWatch

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

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

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

3.36.1 Resource Objects

Any Windows computer

3.36.2 Default Schedule

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

3.36.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the PropertyWatch job fails. The default is 35.
Monitor property changes for an object	
LDAP path to the Active Directory object	Specify the LDAP path to the Active Directory object. For example: `LDAP://dc1.netiq.com/CN=Administrator,CN=Users, DC=dc1,DC=netiq,DC=com`

Parameter	How to Set It
Active Directory property name	Specify the name of the Active Directory property you want to monitor for changes. The default is **whenChanged**. Some valid property names are: ◆ **isDeleted**, which indicates whether the object has been deleted. ◆ **modifyTimeStamp**, which indicates whether the object's modification time has changed. ◆ **USNChanged**, which indicates whether the object's Update Sequence Number has changed. ◆ **whenCreated**, which indicates when the object was created. ◆ **allowedChildClasses**, which lists the classes that can be created under the object. ◆ **displayName**, which indicates the object's displayed name. For example, to monitor changes to the modification time stamp for an object, specify the `modifyTimeStamp` property name. The `USNChanged` property provides similar information but uses the USN rather than a timestamp and can be useful for monitoring replicated object properties.
Event Notification	
Raise event if object property has changed?	Select **Yes** to raise an event if the object property changes. The default is Yes.
Event severity when object property has changed	Set the severity level, from 1 to 40, to indicate the importance of an event in which the object property changes. The default is 20.
Data Collection	
Collect data for changes to object property?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns: ◆ 100 -- no property changes detected, or ◆ 0 -- a property has changed. The default is unselected.

3.37 ReadStat

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

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

- One data stream that records the total read rate. The data detail message describes the percentage of Active Directory reads that are being performed by various services, such as `DRA`, `KCC`, `LSA`, `NSPI`, `SAM`, `XDS`, and `NTDSAPI`.
- One data stream that records the total read rate, but without the detail message breakdown.
- Separate data streams that track the total number of reads per second and the number of reads per second for various services such as `DRA`, `KCC`, `LSA`, `NSPI`, `SAM`, `XDS`, and `NTDSAPI`.

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

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

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

3.37.1 Resource Objects

Active Directory domain controller

3.37.2 Default Schedule

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

3.37.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ReadStat job fails. The default is 35.
Monitor rate of read operations	
Event Notification	
Raise event if read rate exceeds threshold?	Select **Yes** to raise an event if the read rate exceeds the threshold you set. The default is Yes.

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

3.38 ReplEventLog

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

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

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

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

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

3.38.1 Resource Objects

Active Directory domain controller

3.38.2 Default Schedule

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

3.38.3 Setting Parameter Values

Set the following parameters as needed:

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

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

3.39 ReplicationCheckByUSN

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

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

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

3.39.1 Resource Objects

Active Directory domain controller

3.39.2 Default Schedule

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

3.39.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ReplicatonCheckByUSN job fails. The default is 35.
Monitor Active Directory replication by USN	
Event Notification	
Raise event if USN not incremented?	Select **Yes** to raise an event if the USN has not incremented since the last monitoring interval. The default is Yes.
Event severity when USN not incremented	Set the severity level, from 1 to 40, to indicate the importance of an event in which the USN has not incremented since the last monitoring interval. The default is 5.
Data Collection	

Parameter	How to Set It
Collect data for replication status?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns: ◆ 100 -- replication is successful, or ◆ 0 -- the USN has not been updated and replication appears to be stale The default is unselected.

3.40 ReplicationLatency

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

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

For an environment with fewer than 30 domain controllers, you can allow this script to periodically inject a small change in the Active Directory partitions representing every DC and measure how long it takes to replicate that change to other DCs. For environments with thousands of DCs, this script allows even these large Active Directory topologies to get replication latency data with virtually no data overhead. For more information, see Section 3.40.4, “Examples of How this Script Is Used: Example 1,” on page 94.

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

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

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

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

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

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

3.40.1 Resource Objects

Active Directory domain controller.

3.40.2 Default Schedule

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

3.40.3 Setting Parameter Values

Set the following parameters as needed:

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

Parameter	How to Set It
Change/monitor domain partition?	Select **Yes** to monitor the domain partition. The default is Yes.
Change/monitor configuration partition?	Select **Yes** to monitor the configuration partition. The default is unselected.
Change/monitor application partitions?	Select **Yes** to monitor application partitions. The default is Yes.
Monitor global catalog partitions?	Select **Yes** to monitor global catalog partitions. The default is Yes.

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

Container name	Supply a name for a container that will be created in each of the partitions you selected for monitoring above. **NOTE:** You can specify a parent container, however you must first create that parent container with the appropriate security rights to allow creation of sub-objects using the credentials of the AppManager agent (by default) or the credentials you specified for the *Username* and *Password* parameters. The default container name is `AMReplicationLatencyObjects`.
Event Notification	
Raise event if latency threshold exceeded?	Select **Yes** to raise an event if the amount of intersite replication latency exceeds the threshold you set. The default is Yes.
Threshold -- Maximum intersite latency	Specify the maximum amount of intersite replication latency that can be measured before an event is raised. The default is 540 minutes.
Threshold -- Maximum intrasite latency	Specify the maximum amount of intrasite replication latency that can be measured before an event is raised. The default is 15 minutes.
Event severity when latency exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which intersite or intrasite latency exceeds the thresholds you set. The default is 10.
Raise event if time skew detected?	Select **Yes** to raise an event if the creation time of an object used for replication latency monitoring appears to be earlier than the time of the corresponding monitoring job. The default is Yes. **NOTE:** If you notice this event, verify that the report servers are synchronized to a common time source.
Event severity when time skew detected	Set the severity level, from 1 to 40, to indicate the importance of an event in which object creation time is out of sync with the monitoring job.The default is 10.

Parameter	How to Set It
Raise event if object not updated within threshold time?	Select **Yes** to raise an event if an object is not updated within the threshold interval, which indicates that replication is not occurring. The default is Yes. **NOTE:** If you stop a server from injecting changes, delete the replication objects that represent it.
Threshold -- Maximum time for object to be updated	Specify the maximum amount of time that can be taken for an object update to be completed before an event is raised. The default is 24 hours.
Event severity when object not updated within threshold time	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the time it takes to update an object exceeds the threshold. The default is 10.
Data Collection	
Collect data for replication latency?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the replication latency in minutes. The default is unselected. If enabled, data streams are generated indicating the latency of the injected objects for all of the selected partitions to be monitored. **NOTE:** This parameter is only valid if you selected **Monitor** or **Both** for the *Role* parameter.
Collect data for lost data due to latency?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of lost changes. The default is unselected.

3.40.4 Examples of How this Script Is Used: Example 1

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

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

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

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

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

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

3.40.5 Examples of How this Script Is Used: Example 2

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

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

3.40.6 Examples of How this Script Is Used: Example 3

Extending the example introduced in Section 3.40.4, “Examples of How this Script Is Used: Example 1,” on page 94 to a very large Active Directory topology, the ReplicationLatency script could be used to selectively inject changes at a few key sites, while measuring changes at all the remote sites.

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

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

3.41 ReplQueueLen

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

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

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

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

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

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

Performance Objects	Counter
NTDS DirectoryServices	DRA Pending Replication Synchronizations

3.41.1 Resource Objects

Active Directory domain controller

3.41.2 Default Schedule

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

3.41.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ReplQueueLen job fails. The default is 35.
Monitor replication synchronization request queue	
Event Notification	
Raise event if queue length exceeds threshold?	Select **Yes** to raise an event if the length of the replication queue exceeds the threshold you set. The default is Yes.
Threshold -- Maximum unprocessed requests in queue	Specify the maximum number of replication synchronization requests that can be pending in the queue before an event is raised. The default is 12 queued requests.
Event severity when queue length exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the length of the replication queue exceeds the threshold. The default is 20.
Data Collection	
Collect data for replication request queue length?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns the number of pending synchronization requests. The default is unselected.

3.42 ReplSysVol

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

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

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

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

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

3.42.1 Resource Objects

Active Directory domain controller

3.42.2 Default Schedule

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

3.42.3 Setting Parameter Values

Set the following parameters as needed:

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

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

3.43 ResponseTime

Use this Knowledge Script to monitor the time it takes for the target computer to connect to and read the properties of a specific object on an Active Directory domain controller. This script raises an event if the connection or read time exceeds the threshold you set.

Increases in response time may indicate problems in Active Directory configuration.

TIP: Review response-time charts regularly to determine whether response time is trending as expected. Failure to monitor response time can lead to a wide range of problems, including very slow login times and Exchange timeouts.

3.43.1 Resource Objects

Active Directory domain controller

3.43.2 Default Schedule

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

3.43.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ResponseTime job fails. The default is 35.
Monitor connection and read response times	
LDAP path to object on target domain controller	Enter the LDAP (Lightweight Directory Access Protocol) path to an object on the target Active Directory domain controller. The default is `LDAP://server.netiq.com/RootDSE`.
Object property to read	Specify a property of the above object that you want Active Directory to read. Valid properties depend on the object you are requesting. The default is `serverName`.
Event Notification	
Raise event if response time exceeds threshold?	Select **Yes** to raise an event if response time exceeds the threshold you set. The default is Yes.
Threshold -- Maximum connection time	Specify the maximum number of milliseconds allowed to connect to the Active Directory domain controller before an event is raised. The default is 1000 milliseconds.
Threshold -- Maximum read time	Specify the maximum number of milliseconds allowed to read the property value before an event is raised. The default is 1000 milliseconds.
Event severity when response time exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which response time exceeds the threshold. The default is 15.
Data Collection	
Collect data for response times?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns two data streams, one for the connection time and one for the read time. The default is unselected.

3.44 SearchStat

Use this Knowledge Script to monitor the number of Active Directory search operations per second. If the search rate exceeds the threshold you set, an event is raised.

If you use this script to collect data, use the *Data collection mode* parameter to choose what is included in the data stream and data detail message:

- One data stream that records the total search rate. The data detail message describes the percentage of Active Directory searches that are being performed by various services, such as `DRA`, `KCC`, `LDAP`, `LSA`, `NSPI`, `SAM`, `XDS`, `NTDSAPI`.

- One data stream that records the total search rate, but without the detail message breakdown.
- Data streams that track the total number of searches per second and the number of searches per second for various services independently, such as data streams for the search rate of `DRA`, `KCC`, `LDAP`, `LSA`, `NSPI`, `SAM`, `XDS`, and `NTDSAPI`.

If you collect data, keep in mind that the more data streams and detail you collect, the greater the impact on your database management system and overall performance. For example, if you choose the third data collection option, consider adjusting your archive policies or increase the frequency at which you check the size of Data tables in the AppManager repository.

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

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

3.44.1 Resource Objects

Active Directory domain controller

3.44.2 Default Schedule

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

3.44.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	

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 SearchStat job fails. The default is 35.
Monitor rate of search operations	
Event Notification	
Raise event if search rate exceeds threshold?	Select **Yes** to raise an event if the number of search operations per second exceeds the threshold you set. The default is Yes.
Threshold -- Maximum search rate	Specify the maximum number of Active Directory search operations allowed per second before an event is raised. The default is 1 search per second.
Event severity when search rate exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of search operations per second exceeds the threshold. The default is 20.
Data Collection	
Collect data for search rate?	Select **Yes** to collect data for charts and reports. If you enable data collection, specify the data collection mode to use in the *Data collection mode* parameter. The default is unselected.
Data collection mode	Specify the type of data you want to collect. The following entries are valid: ◆ 1 -- one data stream that records the total search rate (searches/second). The data detail message describes the percentage of Active Directory search operations that are performed by various services. ◆ 2 -- one data stream that records the total search rate without any detail message. ◆ 3 -- several data streams: total search rate for all Active Directory services, and one data stream for each separate service. The default is 1 (one data stream and detail message).

3.45 ServerHealth

Use this Knowledge Script to monitor the health of an Active Directory domain controller.

By default, this script checks to see if essential Active Directory services are installed and/or running. You can also monitor the optional DNS server service, and you can disable monitoring of any essential service.

This script using the WMI (Windows Management Instrumentation) replication provider service to check for error conditions related to replication, and uses the WMI Trustmon provider service to verify trust relationships between domains. The WMI Trustmon provider service was introduced in Windows Server 2003 and is not available in earlier versions of Windows. This script raises an event if the WMI Trustmon provider service is not installed. The event provides information on how to install the WMI provider.

You can configure events of varying severity levels to identify critical conditions, error conditions, warning conditions, and informational conditions. You can also set thresholds for the maximum time that can elapse between successful replications and the maximum consecutive number of synchronization failures.

3.45.1 Resource Objects

Active Directory domain controller

3.45.2 Default Schedule

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

3.45.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the ServerHealth job fails. The default is 35.
Monitor essential services?	
Services	
DNS Client	Select **Yes** to monitor the health of the DNS Client service. The default is Yes.
DNS Server	Select **Yes** to monitor the health of the DNS Server service. The default is Yes.
Event Log	Select **Yes** to monitor the health of the Event Log service. The default is Yes.
File Replication Service	Select **Yes** to monitor the health of the File Replication Service (FRS) service. The default is Yes.
Intersite Messaging	Select **Yes** to monitor the health of the Intersite Messaging service. The default is Yes.
Kerberos Key Distribution Center	Select **Yes** to monitor the health of the Kerberos Key Distribution Center (KDC) service. The default is Yes.
Net Logon	Select **Yes** to monitor the health of the Net Logon service. The default is Yes.
Server	Select **Yes** to monitor the health of the Server service. The default is Yes.
Windows Management Instrumentation (for monitoring)	Select **Yes** to monitor the health of the Windows Management Instrumentation (WMI) service. The default is Yes.
Windows Time	Select **Yes** to monitor the health of the Windows Time service. The default is Yes.
Workstation	Select **Yes** to monitor the health of the Workstation service. The default is Yes.
Event Notification	
Raise event if service is installed but not running?	Select **Yes** to enable events if the monitored service is installed but has not been started. The default is Yes.
Event severity when service not running	Set the severity level, from 1 to 40, to indicate the importance of an event in which the monitored service is installed but has not been started. The default is 10.
Monitor Active Directory replication?	

Parameter	How to Set It
Event Notification	
Raise event if WMI replication provider not installed?	Select **Yes** to raise an event if the WMI Active Directory replication provider service is not found. The default is Yes.
Event severity when WMI replication provider not installed	Set the severity level, from 1 to 40, to indicate the importance of an event in which the WMI Active Directory replication provider service is not found. The default is 30.
Raise event if replication is not healthy?	Select **Yes** to raise an event if replication error conditions are detected. The default is Yes.
Error threshold -- Maximum time since last successful replication	Specify the maximum number of days that can elapse since the last successful replication occurred. If the threshold is exceeded, an event is raised. The default is 3 days.
Warning threshold -- Maximum consecutive sync failures	Specify the maximum number of synchronization failures that can occur before an event is raised. The default is 3 failures.
Event severity for critical error event	Set the severity level, from 1 to 40, to indicate the importance of an event in which a condition is detected that constitutes a critical error. The default is 5. An event is always raised if a critical error is detected.
Event severity for Error event	Set the severity level, from 1 to 40, to indicate the importance of an event in which a medium-severity event condition is detected. The default is 10.
Event severity for Warning event	Set the severity level, from 1 to 40, to indicate the importance of an event in which a high-severity event condition is detected. The default is 20.
Raise event if replication is healthy?	Select **Yes** to raise an event if no replication error conditions are detected. The default is unselected.
Event severity for Information event	Set the severity level, from 1 to 40, to indicate the importance of an event in which a low-severity event condition is detected. The default is 30.
Monitor trusts?	
Trust verification level	Select the verification level to use for trust verification: **SC_QUERY**, **Password**, or **SC_RESET**. The default is Password. In order for the parameter setting to take effect, restart the WMI service after you run the job for the first time. **Important** Restarting the WMI service can cause Knowledge Script jobs to fail and raise events. Stop any running Knowledge Script jobs before restarting the WMI service.
Event Notification	
Raise event if WMI Trustmon provider is not installed?	Select **Yes** to raise an event if the WMI Trustmon provider service cannot be found. The default is Yes.
Event severity when WMI Trustmon provider not installed	Set the severity level, from 1 to 40, to indicate the importance of an event in which the WMI Trustmon provider service cannot be found. The default is 30.
Raise event if Windows trust in error?	Select **Yes** to raise an event if an error is found in the Windows trust. The default is Yes.

Parameter	How to Set It
Event severity when Windows trust in error	Set the severity level, from 1 to 40, to indicate the importance of an event in which an error is found in the Windows trust. The default is 10.
Raise event if trusts are found that cannot be monitored?	Select **Yes** to raise an event if trusts are found that cannot be monitored. **NOTE:** The WMI Trustmon provider (installed by default on Windows Server 2003) can only monitor Windows trusts that are inbound-only. Non-Windows trusts cannot be monitored with this script. The default is unselected.
Event severity when trusts not monitored	Set the severity level, from 1 to 40, to indicate the importance of an event in which trusts are found that cannot be monitored. The default is 25.

3.46 SyncRequest

Use this Knowledge Script to monitor the number of failed Active Directory replication synchronization requests from the target server. This script raises an event if the number of synchronization requests that fail per second exceeds the threshold you set.

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

Performance Objects	Counters
NTDS DirectoryServices	The following counters are used to determine the number of failed sync requests: ◆ DRA Sync Requests Made ◆ DRA Sync Requests Successful

The number of failed sync requests is calculated using the following formula:

```
DRA Sync Requests Made - DRA Sync Requests Successful
```

The number of failed sync requests for the current iteration is computed by subtracting the number of failed sync requests at the previous iteration. The percentage of failed synchronization requests since the past iteration is computed and used for threshold comparison.

3.46.1 Resource Objects

Active Directory domain controller

3.46.2 Default Schedule

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

3.46.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the SyncRequest job fails. The default is 35.
Monitor synchronization failure rate?	
Event Notification	
Raise event if sync failure rate exceeds threshold?	Select **Yes** to raise an event if the sync failure rate exceeds the threshold you set. The default is Yes.
Threshold -- Maximum sync failure rate	Specify the maximum percentage of synchronization requests that can have failed since the last script iteration before an event is raised. The default is 90%.
Event severity when sync failure rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the sync failure rate exceeds the threshold. The default is 20.
Data Collection	
Collect data for synchronization failures?	Select **Yes** to collect data for charts and reports. If enabled, data collection returns: ◆ The synchronization failure rate ◆ The total number of synchronization requests made ◆ The number of successful synchronization requests The default is unselected.

3.47 WriteStat

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

If you use this script to collect data, you can choose what is included in the data stream and data detail message:

- One data stream that records the total write rate. The data detail message describes the percentage of Active Directory write operations that are being performed by various services, such as `DRA`, `KCC`, `LDAP`, `LSA`, `NSPI`, `SAM`, `XDS`, and `NTDSAPI`.
- One data stream that records the total write rate, but without the detail message breakdown.
- Data streams that track the total number of write operations per second and the number of writes per second for various services independently, such as `DRA`, `KCC`, `LDAP`, `LSA`, `NSPI`, `SAM`, `XDS`, and `NTDSAPI`.

If you collect data, keep in mind that the more data streams and details you collect, the greater the impact on your database management system and overall performance. For example, if you choose the third data collection option, consider adjusting your archive policies or increase the frequency at which you check the size of Data tables in the AppManager repository.

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

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

3.47.1 Resource Objects

Active Directory domain controller

3.47.2 Default Schedule

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

3.47.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
General Settings	
Raise event if job fails	
Event severity when job fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the WriteStat job fails. The default is 35.
Raise event if write rate exceeds threshold?	Select **Yes** to raise an event if the number of write operations per second exceeds the threshold you set. The default is Yes.
Event Notification	
Threshold -- Maximum write rate	Specify the maximum number of Active Directory write operations allowed per second before an event is raised. The default is 1 write operation per second.

Parameter	How to Set It
Event severity when write rate exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the number of write operations per second exceeds the threshold. The default is 20.
Data Collection	
Collect data for write rate?	Select **Yes** to collect data for charts and reports. If enabled, specify the data collection mode to use in the *Data collection mode* parameter. The default is unselected.
Data collection mode	Specify the type of data you want to collect. The following entries are valid: ◆ 1 -- one data stream that records the total search rate (searches/second). The data detail message describes the percentage of Active Directory search operations that are performed by various services. ◆ 2 -- one data stream that records the total search rate without any detail message. ◆ 3 -- several data streams: total search rate for all Active Directory services, and one data stream for each separate service. The default is 1 (one data stream and detail message).

3.48 AD Knowledge Script Groups

The following Knowledge Script Groups (KSGs) are installed as part of the installation of AppManager for Active Directory. Like other Knowledge Scripts for monitoring Active Directory, they are located on the AD Knowledge Script tab. However, they are also accessible from the RECOMMENDED Knowledge Script tab.

3.48.1 Tips for Using Knowledge Script Groups

The AD KSGs contain a recommended subset of Active Directory scripts that represent a “best practices” usage of AppManager for monitoring Active Directory in your organization. These KSGs can be used with AppManager monitoring policies. A monitoring policy, which you can use to efficiently and consistently monitor all of 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 the topic titled “About policy-based monitoring” in the AppManager Help.

Generally, each of the KSGs is intended to be used only in the role that is specified as part of the description of the group, with the exception of the AD KSG. Unlike the others, the AD KSG leverages the Knowledge Script job delegation feature included with AppManager for Active Directory 6.2.

Whereas the recommended KSGs are designed to be deployed only on the Domain Controllers listed in the description of each group, the AD KSG executes only on role-holding Domain Controllers. The AD KSG should be used as an alternative to all the others; that is, you should either use the AD KSG or each of the separate KSGs as designated.

KSGs are composed of selected scripts from the regular Knowledge Script tabs. When you modify a script, keep in mind that the script that belongs to a KSG is a different copy of the actual script you access from the **AD** tab. The changes you make are not reflected in the script that is part of the KSG.

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, such as a single domain or an entire forest.

If you modify or remove a script associated with one of these RECOMMENDED KSGs and want to restore it to its original form, you can either reinstall AppManager for Active Directory on the repository computer or check in the appropriate script from the `qdb\kp\ad\<Knowledge Script Group name>` directory.

3.49 AD

Deploy this Knowledge Script Group (KSG) to all domain controllers you want to monitor. This comprehensive KSG has the job delegation feature enabled for Knowledge Scripts that support this feature. If you use this KSG, avoid using the other recommended KSGs that do not employ the job delegation feature. For more information about job delegation, see Section 3.1, “AD Knowledge Script Job Delegation,” on page 27.

The AD KSG contains the following scripts:

Knowledge Script	Default Settings Changed for Use in Knowledge Script Group
Authentications	◆ Collect data for Kerberos authentications? (enabled) ◆ Collect data for NTLM authentications? (enabled)
BridgeheadChange	◆ Enable job delegation? (enabled)
ClientSessions	◆ Collect data for number of client sessions? (enabled) ◆ Threshold -- Maximum number of client sessions (250)
DatabaseSize	◆ Collect data for database disk space usage? (enabled) Advanced Option (**Advanced** Properties tab): ◆ Collect data every 96 job iterations. Calculate Average.
DCAdvertised	None.
DCHealthMonitor	◆ Collect data for DC health? (enabled) Advanced Option (**Advanced** Properties tab): ◆ Collect data every 12 job iterations. Calculate Average.
DCInSiteConnectivity	◆ Enable job delegation? (enabled)
DomainConnectivity	◆ Enable job delegation? (enabled)
EnumerateSites	◆ Enable job delegation? (enabled)
EventLog	◆ Filter -- Source (`NTDS KCC`)
EventLog (NetLogon)	None.
EventLog (W32Time)	None.
FSMOChange	◆ Enable job delegation? (enabled)
FSMOHealth	◆ Enable job delegation? (enabled)
FSMOPlacement	◆ Enable job delegation? (enabled)
GlobalCatalogChange	◆ Enable job delegation? (enabled)

Knowledge Script	Default Settings Changed for Use in Knowledge Script Group
GlobalCatalogHealth	◆ Enable job delegation? (enabled) ◆ Collect data for global catalog status? (enabled)
KCCConnections	None.
KCCDisabled	Enable job delegation? (enabled)
KDCRequests	None.
NumberOfObjects	◆ Enable job delegation? (enabled) ◆ Object class to check (* for all classes) (*) ◆ Raise event if number of objects exceeds threshold? (enabled) ◆ Collect data for number of objects? (enabled) ◆ Number of objects to return (0 for all objects) (1)
NumberOfUsersLocked	◆ Enable job delegation? (enabled) ◆ Collect data for number of locked user accounts? (enabled)
ReplEventLog	None.
ReplSysVol	None.
ResponseTime	◆ Collect data for response times? (enabled) Advanced Option (**Advanced** Properties tab): ◆ Collect data every 12 job iterations. Calculate Average.
ServerHealth	None.
SyncRequest	None.

3.50 AD (all DCs)

Deploy this Knowledge Script Group (KSG) to all domain controllers you want to monitor. This KSG contains the following scripts:

Knowledge Script	Default Settings Changed for Use in Knowledge Script Group
Authentications	◆ Collect data for Kerberos authentications? (enabled) ◆ Collect data for NTLM authentications? (enabled
ClientSessions	◆ Collect data for number of client sessions? (enabled) ◆ Threshold -- Maximum number of client sessions (250)
DatabaseSize	◆ Collect data for database disk space usage? (enabled) Advanced Option (**Advanced** Properties tab): ◆ Collect data every 96 job iterations. Calculate Average.
DCAdvertised	None.

Knowledge Script	Default Settings Changed for Use in Knowledge Script Group
DCHealthMonitor	◆ Collect data for DC health? (enabled) Advanced Option (**Advanced** Properties tab): ◆ Collect data every 12 job iterations. Calculate Average.
DCInSiteConnectivity	None.
EventLog (NetLogon)	None.
EventLog (W32Time)	None.
EventLog	Filter -- Source (`NTDS KCC`)
KCCConnections	None.
KDCRequests	None.
ReplEventLog	None.
ReplSysVol	None.
ResponseTime	◆ Collect data for response times? (enabled) Advanced Option (**Advanced** Properties tab): ◆ Collect data every 12 job iterations. Calculate Average.
ServerHealth	None.
SyncRequest	None.

3.51 AD (one DC per domain)

Deploy this Knowledge Script Group (KSG) to a single domain controller per domain. This KSG contains the following scripts:

Knowledge Script	Default Settings Changed for Use in Knowledge Script Group
DomainConnectivity	None.
FSMOChange	None.
FSMOHealth	None.
FSMOPlacement	None.
NumberOfObjects	◆ Object class to check (* for all classes) (*) ◆ Raise event if number of objects exceeds threshold? (enabled) ◆ Collect data for number of objects? (enabled) ◆ Number of objects to return (0 for all objects) (1)
NumberOfUsersLocked	◆ Collect data for number of locked user accounts? (enabled)

3.52 AD (one DC per forest)

Deploy this Knowledge Script Group (KSG) to a single domain controller per forest. This KSG contains the following scripts:

Knowledge Script	Default Settings Changed for Use in Knowledge Script Group
BridgeheadChange	None.
EnumerateSites	None.
GlobalCatalogChange	None.

3.53 AD (one DC per site)

Deploy this Knowledge Script Group (KSG) to a single domain controller per site. This KSG contains the following scripts:

Knowledge Script	Default Settings Changed for Use in Knowledge Script Group
GlobalCatalogHealth	Collect data for global catalog status? (enabled)
KCCDisabled	None.

4 ReportADSI Knowledge Scripts

The ReportADSI category provides the following templates for generating reports based on data in Active Directory. From within the Operator Console, you can select one of the AppManager for Microsoft Active Directory in the Knowledge Script pane and press **F1** for complete details.

Report Script	Report Contents
ADObjects	Summarizes the properties and related values of objects in an Active Directory domain.
GroupMembership	Summarizes all the members that belong to an Active Directory group.
LocalService	Summarizes the services running on a managed computer in an Active Directory domain.
LocalUser	Summarizes the local user accounts on a managed computer in an Active Directory domain.
ReplicationLatency	Generates a report about Active Directory replication latency.
ReplSysVol	Reports on the consistency of files in the SysVol folder of the Report Agent's corresponding domain controller and the SysVol folders of that domain controller's replication partners.
ServerRoles	Summarizes the Active Directory roles for each server in the forest.
UserAccountsDisabled	Generates a report listing disabled and locked accounts in an Active Directory domain.
UserBadPasswordCount	Summarizes the number of failed logins due to bad passwords for accounts in an Active Directory domain.
UserMemberOfMoreThanOneGroup	Summarizes the number of members that belong to more than one group in an Active Directory domain.
UserPasswordExpired	Summarizes the number of accounts with expired passwords in an Active Directory domain.

4.1 ADObjects

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

4.1.1 Resource Object

Report Agent > Active Directory > <Active Directory domain>

4.1.2 Default Schedule

The default schedule is **Run once**.

4.1.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Source	
Select OU or CN name	Click **Browse [...]** to select the organizational unit or common name object for which you want to create a report.
Report Settings	
Include table of parameter values?	Set to **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.
Add job ID to output folder name?	Set to **Yes** to append the job ID to the name of the output folder. The default is unchecked. A job ID helps make the correlation between a specific instance of a Report Script and the corresponding report.
Report properties	Click **Browse [...]** to set report properties as desired.
Add timestamp to title?	Set to **Yes** to append a timestamp to the title of the report, making each title unique. The default is unchecked. The timestamp is made up of the date and time the report was generated. By adding a timestamp, you can run consecutive iterations of the same report without overwriting previous output.
Include Error Table?	Set to **Yes** to include a table in the report that lists any errors encountered when running the report. The default is Yes.
Omit property when value not found?	Set to **Yes** to omit any properties that do not have a value specified. The default is Yes.
ADsPath link address	Specifies the default Microsoft MSDN URL for ADsPath information. This link is provided in the report for reference purposes.
Class link address	Specifies the default Microsoft MSDN URL for Class information. All classes referenced in the report are associated with hyperlinks based upon this URL.
Property link address	Specifies the default Microsoft MSDN URL for Property information. All properties referenced in the report are associated with hyperlinks based upon this URL.
Schema link address	Specifies the default Microsoft MSDN URL for Schema information. This link is provided in the report for reference purposes.
Event Notification	
Raise event for report success?	Set to **Yes** to raise an event when the report is successfully generated. The default is unchecked.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).

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

4.2 GroupMembership

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

4.2.1 Resource Object

Report Agent > Active Directory > <Active Directory domain>

4.2.2 Default Schedule

The default schedule is **Run once**.

4.2.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Source	
Select OU or CN name	Click **Browse [...]** to select the organizational unit or common name object for which you want to create a report.
Report Settings	
Include table of parameter settings?	Set to **Yes** to include a table in the report that lists parameter settings for the report script. The default is unchecked.
Output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.
Add job ID to output folder name?	Set to **Yes** to append the job ID to the name of the output folder. The default is unchecked. A job ID helps make the correlation between a specific instance of a Report Script and the corresponding report.
Report properties	Click **Browse [...]** to set report properties as desired.

Description	How to Set It
Add timestamp to title?	Set to **Yes** to append a timestamp to the title of the report, making each title unique. The default is unchecked. The timestamp is made up of the date and time the report was generated. By adding a timestamp, you can run consecutive iterations of the same report without overwriting previous output.
Include Error Table?	Set to **Yes** to include a table in the report that lists any errors encountered when running the report. The default is Yes.
Event Notification	
Raise event for report success?	Set to **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated but contains no data. The default is 25 (blue event indicator).
Event severity for report with error(s)	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated with some errors. The default is 15 (yellow event indicator).
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (magenta event indicator).

4.3 LocalService

Use this Knowledge Script list the services running on a managed computer in an Active Directory domain.

4.3.1 Resource Object

Report Agent > Active Directory > <Active Directory domain>

4.3.2 Default Schedule

The default schedule is **Run once**.

4.3.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Source	
Target computer	Click **Browse [...]** to select the computer whose Active Directory services the report will list.

Description	How to Set It
Report Settings	
Include table of parameter settings?	Set to **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.
Add job ID to output folder name?	Set to **Yes** to append the job ID to the name of the output folder. The default is unchecked. A job ID helps make the correlation between a specific instance of a Report Script and the corresponding report.
Report properties	Click **Browse [...]** to set report properties as desired.
Add timestamp to title?	Set to **Yes** to append a timestamp to the title of the report, making each title unique. The default is unchecked. The timestamp is made up of the date and time the report was generated. By adding a timestamp, you can run consecutive iterations of the same report without overwriting previous output.
Include Error Table?	Set to **Yes** to include a table in the report that lists any errors encountered when running the report. The default is Yes.
ADsPath link address	Specifies the default Microsoft MSDN URL for ADsPath information. This link is provided in the report for reference purposes.
Class link address	Specifies the default Microsoft MSDN URL for Class information. All classes referenced in the report are associated with hyperlinks based upon this URL.
Property link address	Specifies the default Microsoft MSDN URL for Property information. All properties referenced in the report are associated with hyperlinks based upon this URL.
Schema link address	Specifies the default Microsoft MSDN URL for Schema information. This link is provided in the report for reference purposes.
Event Notification	
Raise event for report success?	Set to **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated but contains no data. The default is 25 (blue event indicator).
Event severity for report with error(s)	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated with some errors. The default is 15 (yellow event indicator).
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (magenta event indicator).

4.4 LocalUser

Use this Knowledge Script list the local user accounts on a managed computer in an Active Directory domain.

4.4.1 Resource Object

Report Agent > Active Directory > <Active Directory domain>

4.4.2 Default Schedule

The default schedule is **Run once**.

4.4.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Source	
Target computer	Click **Browse [...]** to select the computer that is the subject of your report.
Report Settings	
Include table of parameter settings?	Set to **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.
Add job ID to output folder name?	Set to **Yes** to append the job ID to the name of the output folder. The default is unchecked. A job ID helps make the correlation between a specific instance of a Report Script and the corresponding report.
Report properties	Click **Browse [...]** to set report properties as desired.
Add timestamp to title?	Set to **Yes** to append a timestamp to the title of the report, making each title unique. The default is unchecked. The timestamp is made up of the date and time the report was generated. By adding a timestamp, you can run consecutive iterations of the same report without overwriting previous output.
Include Error Table?	Set to **Yes** to include a table in the report that lists any errors encountered when running the report. The default is Yes.
ADsPath link address	Specifies the default Microsoft MSDN URL for ADsPath information. This link is provided in the report for reference purposes.
Class link address	Specifies the default Microsoft MSDN URL for Class information. All classes referenced in the report are associated with hyperlinks based upon this URL.
Property link address	Specifies the default Microsoft MSDN URL for Property information. All properties referenced in the report are associated with hyperlinks based upon this URL.

Description	How to Set It
Schema link address	Specifies the default Microsoft MSDN URL for Schema information. This link is provided in the report for reference purposes.
Event Notification	
Raise event for report success?	Set to **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated but contains no data. The default is 25 (blue event indicator).
Event severity for report with error(s)	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated with some errors. The default is 15 (yellow event indicator).
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (magenta event indicator).

4.5 ReplicationLatency

Use this Knowledge Script to report on Active Directory replication latency. This script summarizes the average, maximum, and minimum values of the data streams collected by the AD_ReplicationLatency Knowledge Script, or another script you select, within the time range you select.

4.5.1 Resource Object

Report Agent > Active Directory

4.5.2 Default Schedule

The default schedule is **Run once**.

4.5.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select computer(s)	Click **Browse [...]** to select the computers for your report.
Select time range	Click **Browse [...]** to set a specific or sliding time range for data included in your report.
Select peak weekday(s)	Click **Browse [...]** to select the days of the week to include in your report.

Description	How to Set It
Aggregation interval	Select the time interval by which the data in your report is aggregated. Possible values range from 1 to 90 hours. Default is 1 hour.
Report Settings	
Include table of parameter settings?	Set to **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Include table?	Set to **Yes** to include a table of data stream values in the report. The default is Yes.
Include chart?	Set to **Yes** to include a chart of data stream values in the report. The default is unchecked.
Select chart style	Click **Browse [...]** to define the graphic properties of the charts in your report.
Series style (Average)	Select a graphical style for the average value series in the chart. The default value is Line.
Chart title	Enter a title to assign to the chart of values.
Select output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.
Add job ID to output folder name?	Set to **Yes** to append the job ID to the name of the output folder. The default is unchecked. A job ID helps make the correlation between a specific instance of a Report Script and the corresponding report.
Select properties	Click **Browse [...]** to set report properties as desired.
Add timestamp to title?	Set to **Yes** to append a timestamp to the title of the report, making each title unique. The default is unchecked. The timestamp is made up of the date and time the report was generated. By adding a timestamp, you can run consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event for report success?	Set to **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated but contains no data. The default is 25 (blue event indicator).
Event severity for report with error(s)	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated with some errors. The default is 15 (yellow event indicator).
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (magenta event indicator).

4.6 ReplSysVol

Use this Knowledge Script to display information about the consistency of files in the SysVol folder of the Report agent's corresponding domain controller and the files in the SysVol folders of any replication partners of that domain controller.

You can return a list of all files whose content does not match.

The report lists each replication partner, and for each partner, the following columns of information:

- **File Compare**. If all files in the SysVol folder also exist on the replication partner, a value of `OK` is displayed in this column. Any files that exist in the SysVol folder but do not exist on the replication partner are listed here.
- **File Size Match**. If all matching files in the SysVol folder and the replication partner's SysVol folder match in size, a value of `OK` is displayed in this column. Any files with a disparity in size are listed here.
- **File Content Match**. If you enable the *Discover all files that do not match file content* parameter and all files match for content, a value of `OK` is displayed in this column. If any files do not match for content, those files are listed here.

  If you disable the *Discover all files that do not match file content*

  parameter and all files match for content, a value of `OK` is displayed in this column. If a non-matching file is found, comparison of file content stops with that file, and a value of `Testing Stopped` is displayed in this column.

4.6.1 Resource Object

Report Agent > Active Directory > <Active Directory domain>

4.6.2 Default Schedule

The default schedule is **Run once**.

4.6.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Discover all files that do not match file content?	Set to **Yes** to return a list of all files in the replication partner's SysVol folder whose content is different than the content of matching files in the SysVol folder of the Report Agent's corresponding domain controller. The default is Yes.
Report Settings	
Include table of parameter settings?	Set to **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.

Description	How to Set It
Add job ID to output folder name?	Set to **Yes** to append the job ID to the name of the output folder. The default is unchecked. A job ID helps make the correlation between a specific instance of a Report Script and the corresponding report.
Report properties	Click **Browse [...]** to set report properties as desired.
Add timestamp to title?	Set to **Yes** to append a timestamp to the title of the report, making each title unique. The default is unchecked. The timestamp is made up of the date and time the report was generated. By adding a timestamp, you can run consecutive iterations of the same report without overwriting previous output.
Include Error Table?	Set to **Yes** to include a table in the report that lists any errors encountered when running the report. The default is Yes.
Event Notification	
Raise event for report success?	Set to **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated but contains no data. The default is 25 (blue event indicator).
Event severity for report with error(s)	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated with some errors. The default is 15 (yellow event indicator).
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (magenta event indicator).

4.7 ServerRoles

Use this Knowledge Script to display the Active Directory roles for each server in the forest. Active Directory roles include FSMO, Global Catalog, Bridgehead, and Inter-Site Topology Generator.

4.7.1 Resource Object

Report Agent > Active Directory > <Active Directory domain>

4.7.2 Default Schedule

The default schedule is **Run once**.

4.7.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Source	
Include forest domain naming master?	Set to **Yes** to include the forest domain naming master in the report. The default is Yes.
Include forest schema master?	Set to **Yes** to include the forest schema master in the report. The default is Yes.
Include domain infrastructure masters?	Set to **Yes** to include domain infrastructure masters in the report. The default is Yes.
Include domain PDC emulators?	Set to **Yes** to include domain PDC emulators in the report. The default is Yes.
Include domain RID masters?	Set to **Yes** to include domain RID masters in the report. The default is Yes.
Include global catalogs?	Set to **Yes** to include global catalogs in the report. The default is Yes.
Include bridgeheads?	Set to **Yes** to include bridgeheads in the report. The default is Yes.
Include Inter-Site Topology Generators (ISTG)?	Set to **Yes** to include Inter-Site Topology Generators in the report. The default is Yes.
Report Settings	
Include table of parameter settings?	Set to **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.
Add job ID to output folder name?	Set to **Yes** to append the job ID to the name of the output folder. The default is unchecked. A job ID helps make the correlation between a specific instance of a Report Script and the corresponding report.
Report properties	Click **Browse [...]** to set report properties as desired.
Add timestamp to title?	Set to **Yes** to append a timestamp to the title of the report, making each title unique. The default is unchecked. The timestamp is made up of the date and time the report was generated. By adding a timestamp, you can run consecutive iterations of the same report without overwriting previous output.
Include Error Table?	Set to **Yes** to include a table in the report that lists any errors encountered when running the report. The default is Yes.
Event Notification	
Raise event for report success?	Set to **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).

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

4.8 UserAccountsDisabled

Use this Knowledge Script to generate a report listing disabled and locked accounts in an Active Directory domain. The report contains information for the selected organizational unit or common name object and for all sub-objects.

4.8.1 Resource Object

Report Agent > Active Directory > <Active Directory domain>

4.8.2 Default Schedule

The default schedule is **Run once**.

4.8.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data source	
Select OU or CN name	Click **Browse [...]** to select the organizational unit or common name object for which you want to create a report.
Select object classes	Indicates the object classes to include for the selected organizational unit or common name object. The default is computer and user.
Report Settings	
Include table of parameter settings?	Set to **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.
Add job ID to output folder name?	Set to **Yes** to append the job ID to the name of the output folder. The default is unchecked. A job ID helps make the correlation between a specific instance of a Report Script and the corresponding report.

Description	How to Set It
Report properties	Click **Browse [...]** to set report properties as desired.
Add timestamp to title?	Set to **Yes** to append a timestamp to the title of the report, making each title unique. The default is unchecked. The timestamp is made up of the date and time the report was generated. By adding a timestamp, you can run consecutive iterations of the same report without overwriting previous output.
Include Error Table?	Set to **Yes** to include a table in the report that lists any errors encountered when running the report. The default is Yes.
Event Notification	
Raise event for report success?	Set to **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated but contains no data. The default is 25 (blue event indicator).
Event severity for report with error(s)	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated with some errors. The default is 15 (yellow event indicator).
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (magenta event indicator).

4.9 UserBadPasswordCount

Use this Knowledge Script to list the number of failed logins due to bad passwords for accounts in an Active Directory domain. You can set a threshold for the maximum number of login failures due to bad passwords. Any account that exceeds the threshold you set is included in the report. The report contains information for the selected organizational unit or common name object and for all sub-objects.

4.9.1 Resource Object

Report Agent > Active Directory > <Active Directory domain>

4.9.2 Default Schedule

The default schedule is **Run once**.

4.9.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Source	
Select OU or CN name	Click **Browse [...]** to select the organizational unit or common name object for which you want to create a report.
Select object classes	Indicates the object classes to include for the selected organizational unit or common name object. The default is computer and user.
Threshold -- Maximum number of login failures due to bad passwords	Specify a threshold for the number of login failures due to bad password attempts. Any user account that exceeds this threshold is included in the report. The default is 0.
Report Settings	
Include table of parameter settings?	Set to **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.
Add job ID to output folder name?	Set to **Yes** to append the job ID to the name of the output folder. The default is unchecked. A job ID helps make the correlation between a specific instance of a Report Script and the corresponding report.
Report properties	Click **Browse [...]** to set report properties as desired.
Add timestamp to title?	Set to **Yes** to append a timestamp to the title of the report, making each title unique. The default is unchecked. The timestamp is made up of the date and time the report was generated. By adding a timestamp, you can run consecutive iterations of the same report without overwriting previous output.
Include Error Table?	Set to **Yes** to include a table in the report that lists any errors encountered when running the report. The default is Yes.
Event Notification	
Raise event for report success?	Set to **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated but contains no data. The default is 25 (blue event indicator).
Event severity for report with error(s)	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated with some errors. The default is 15 (yellow event indicator).
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (magenta event indicator).

4.10 UserMemberOfMoreThanOneGroup

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

4.10.1 Resource Object

Report Agent > Active Directory > <Active Directory domain>

4.10.2 Default Schedule

The default schedule is **Run once**.

4.10.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Source	
Select OU or CN name	Click **Browse [...]** to select the organizational unit or common name object for which you want to create a report.
Select object classes	Indicates the object classes to include for the selected organizational unit or common name object. The default is computer and user.
Report settings	
Include table of parameter settings?	Set to **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.
Add job ID to output folder name?	Set to **Yes** to append the job ID to the name of the output folder. The default is unchecked. A job ID helps make the correlation between a specific instance of a Report Script and the corresponding report.
Report properties	Click **Browse [...]** to set report properties as desired.
Add timestamp to title?	Set to **Yes** to append a timestamp to the title of the report, making each title unique. The default is unchecked. The timestamp is made up of the date and time the report was generated. By adding a timestamp, you can run consecutive iterations of the same report without overwriting previous output.
Include Error Table?	Set to **Yes** to include a table in the report that lists any errors encountered when running the report. The default is Yes.
Event Notification	
Raise event for report success?	Set to **Yes** to raise an event when the report is successfully generated. The default is Yes.

Description	How to Set It
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated but contains no data. The default is 25 (blue event indicator).
Event severity for report with error(s)	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated with some errors. The default is 15 (yellow event indicator).
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (magenta event indicator).

4.11 UserPasswordExpired

Use this Knowledge Script to list the number of accounts with expired passwords in an Active Directory domain. The report contains information for the selected organizational unit or common name object and for all sub-objects.

4.11.1 Resource Object

Report Agent > Active Directory > <Active Directory domain>

4.11.2 Default Schedule

The default schedule is **Run once**.

4.11.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Data Source	
Select OU or CN name	Click **Browse [...]** to select the organizational unit or common name object for which you want to create a report.
Select object classes	Indicates the object classes to include for the selected organizational unit or common name object. The default is computer and user.
Report Settings	
Include table of parameter settings?	Set to **Yes** to include a table in the report that lists parameter settings for the report script. The default is Yes.
Output folder	Click **Browse [...]** to select the name and location of the folder in which the report will be saved.

Description	How to Set It
Add job ID to output folder name?	Set to **Yes** to append the job ID to the name of the output folder. The default is unchecked. A job ID helps make the correlation between a specific instance of a Report Script and the corresponding report.
Report properties	Click **Browse [...]** to set report properties as desired.
Add timestamp to title?	Set to **Yes** to append a timestamp to the title of the report, making each title unique. The default is unchecked. The timestamp is made up of the date and time the report was generated. By adding a timestamp, you can run consecutive iterations of the same report without overwriting previous output.
Include Error Table?	Set to **Yes to** include a table in the report that lists any errors encountered when running the report. The default is Yes.
Event Notification	
Raise event for report success?	Set to **Yes** to raise an event when the report is successfully generated. The default is Yes.
Event severity for report success	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated. The default is 35 (magenta event indicator).
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successfully generated but contains no data. The default is 25 (blue event indicator).
Event severity for report with error(s)	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is generated with some errors. The default is 15 (yellow event indicator).
Event severity for report failure	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (magenta event indicator).