NetIQ® AppManager® for Microsoft Exchange 2000 or 2003

Management Guide

February 2012

Legal Notice

Contents

About this Book and the Library

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

Intended Audience

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

Other Information in the Library

The library provides the following information resources:

Installation Guide for AppManager

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

User Guide for AppManager Control Center

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

Administrator Guide for AppManager

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

Upgrade and Migration Guide for AppManager

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

Management guides

Provide information about installing and monitoring specific applications with AppManager.

Help

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

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

Conventions

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

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

About NetIQ Corporation

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

Contacting Sales Support

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

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

Contacting Technical Support

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

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

Contacting Documentation Support

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

Contacting the Online User Community

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

Chapter 1
Introducing AppManager for Microsoft Exchange 2000 or 2003

AppManager for Microsoft Exchange 2000 or 2003 provides a comprehensive solution for monitoring the performance and availability of your Microsoft Exchange 2000 or Microsoft Exchange Server 2003 environment. With AppManager for Microsoft Exchange 2000 or 2003, you can:

- View the complete messaging structure for your Exchange environment.
- Set thresholds and event severity notification for core Exchange components.
- Troubleshoot system problems, and initiate automated responsive or corrective actions.
- Gather information about Exchange performance and usage for real-time and historical reporting.
- Extend monitoring functionality with easy-to-use Visual Basic for Applications (VBA) scripting tools.
- Run Knowledge Script jobs on Exchange components.
- Run Knowledge Script jobs directly on Exchange virtual servers in a clustered environment.

Chapter 2
Preparing to Install the Module

This chapter describes the requirements you need to address before installing AppManager for Microsoft Exchange 2000 or 2003.

Before you install Microsoft Exchange 2000 or Microsoft Exchange Server 2003, set up the required accounts with the proper credentials for each Exchange Server and each virtual server you want to monitor.

For more information about Exchange administration, see the Microsoft documentation for Exchange 2000 or Server 2003. For more information about preparing to install AppManager, see the *Installation Guide for AppManager*.

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 Microsoft Exchange 2000 or 2003 has the following requirements:

Item	Requirement
NetIQ AppManager installed on the AppManager repository (QDB) computers, on the Exchange 2000 or 2003 server you want to monitor (agents), and on all console computers	7.0 or later
Microsoft operating system running on the managed computer (agent)	Windows Server 2003 R2 (32- and 64-bit)
Microsoft Exchange Server	One of the following versions: • Microsoft Exchange 2000 • Microsoft Exchange Server 2003 In active/passive mode, supports seven EVSs on 8-node clusters, where the number of EVSs is the number of nodes minus one. In active/active mode, supports two nodes and up to eight EVSs.
Accounts/Permissions	Administrator
Microsoft Log Parser	Version 2.2. Required for using the LogParser Knowledge Script.

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

Installing and Configuring the Agent Service

When you ran the AppManager setup program, you were prompted to install the agent. For applications running in a clustered environment, install the agent on all nodes in the cluster.

You need to create a Windows user account to run the agent. The account must be a member of the domain to which the Exchange server belongs. The setup program uses this account as the Log On As account for the `NetIQmc` and `NetIQccm` services.

Exchange Server	Account
Exchange Server	**LocalSystem** or a member of the local **Administrators** group. Can be a local account or a domain user with no additional permissions required.
Exchange Virtual Server	A domain user account with **Local Admin** rights on all nodes in the cluster.

The agent setup does not create the mailbox and profile for the Log On As account. For more information, see "Configuring Exchange Server Mailbox and Profile Information in Security Manager" on page 11.

For more information about updating the agent services, NetIQ AppManager Client Resource Monitor Service (`NetIQmc`) and NetIQ AppManager Client Communication Manager (`netiqccm`), see "Permissions for Running Knowledge Scripts" on page 6.

Monitoring Exchange 2000 or Server 2003 requires you to specify a Log On account for the agent service. There are no special requirements for the Windows account used by the agent unless you want the agent to send MAPI mail as an action. In that case, specify an account that has an Exchange mailbox. For more information, see "Creating a Windows User Account" on page 4.

Note

Do not install an Exchange MAPI client on your Exchange server because of compatibility issues between MAPI clients within Microsoft Office and Microsoft Exchange.

Enabling the Agent to Send MAPI Mail

If you want the agent to send a MAPI mail message as a responsive action, the Log On As account for the agent must also have an enabled Exchange mailbox and profile.

To enable the AppManager agent to send MAPI mail:

1. Install an Exchange client, such as Microsoft Outlook, on the computer where you installed the agent. For more information about installing Exchange clients, see the documentation for Exchange 2000 or Server 2003.
2. Create an Exchange mailbox for the Log On As account used by the agent.

Creating a Windows User Account

The AppManager agent uses an Exchange mailbox to send MAPI mail, and send mail from server to server for each instance of the monitoring service.

`Qexch2k1a` service is the AppManager monitoring service for Exchange 2000 or 2003. You need to configure this service for each Exchange server. For Exchange clusters, configure this service for each Exchange Virtual Server. For example, in a four-node cluster with three EVSs, configure three services as `qexch2k1a, qexch2k2a` and `qexch2k3a`, one for each Exchange Virtual Server. For more information on installing and configuring the module see, "Installing the Module" on page 9 and "Configuring User Account and Mailbox Information for Virtual Servers" on page 12.

If you are creating multiple accounts for use by multiple instances of the monitoring service, configure each account with a mailbox on the server where it will log on.

To create a Windows user account and mailbox for the monitoring service account:

1. From the Microsoft Exchange Start menu, select **All Programs > Active Directory Users and Computers**.
2. Right-click **Users**, select **New**, and then select **User**. Enter the user details in the New Object wizard.
3. Click **Next**. Specify and confirm the password.
4. Select **User cannot change password** and **Password never expires**, and then click **Next**.
5. Select **Create an Exchange mailbox**.

Note
If you are not prompted to create an Exchange mailbox, add the user account from the Exchange server or ensure that the user account you are currently logged on as has Exchange View-Only Administrator permission.

6. Complete the following fields:

Field	Description
Alias	The mailbox alias for the account.
Server	The Exchange server that manages the account mailbox.
Mailbox Store	The mailbox store that contains the account mailbox.

7. Verify the account information, then click **Finish.**

After you create a user account and mailbox, ensure that Active Directory has time to replicate the account information before you attempt to grant additional permissions such as **Log on as a service**. If the user account information is not propagated through Active Directory, granting additional permissions will fail.

To assign the right to log on as a service:

1. From the Control Panel, navigate to Administrative Tools and click **Domain Security Policy** to give the **Log on as a service** permission to the newly created user account.
2. Expand **Local Policies**.
3. Click **User Rights Assignment** and then double-click **Log on a service**.
4. Select **Define these policy settings**.
5. Click **Add User or Group**.
6. Enter the newly created user account.
7. Click **OK**.

Permissions for Running Knowledge Scripts

AppManager for Microsoft Exchange 2000 or 2003 requires either that the NetIQ AppManager Client Resource Monitor (`netiqmc`) and the NetIQ AppManager Client Communication Manager (`netiqccm`) agent services to run using the Local System account or that the user account running the `netiqmc` and the `netiqccm` services must be a member of the following groups:

- Local Administrators group on the Exchange Server
- Exchange View-Only Administrators group

By default, the setup program configures the agent to use the Windows Local System account.

To update the agent services to run under a different account:

1. Navigate to the Services Administrative Tool in the the Administrative Tools folder in the Control Panel.
2. Right-click **NetIQ AppManager Client Communication Manager** 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** service.
6. Restart both services.

The following Exchange Knowledge Scripts require the service account on the managed Exchange Server to be configured with the **Exchange View-Only Administrator** permission:

- Connectivity
- InactiveMailboxes
- InactivePublicFolders
- MailboxesOverStorageLimit
- MailboxesWithoutStorageLimit
- NumberofMailboxes
- PFAclChanges
- PFAclInfo
- PFReplicationByObj
- ResponseTime
- TopNISMailboxRes
- TopNISPublicRes

To set the Exchange View-Only Administrator permission:

1. Start Microsoft Exchange System Manager.
2. Right-click the **organization** level or **administrative group** level and click **Delegate Control**.
3. Add the user account to which you want to delegate control.
4. In the Exchange Administration Delegation Wizard, select the **Exchange View Only Administrator** permission.
5. Click **OK**.

Setting Permissions to Automatically Create an Exchange Mailbox

When you install the agent, you can select the setup option to automatically create an Exchange mailbox.

Each Exchange Server should have a unique mailbox for monitoring purposes. The AppManager for Microsoft Exchange 2000 or 2003 setup program creates the mailbox with the following naming convention: `netiq-<servername>`.

To automatically create the mailbox, the Windows user account in either of the following cases must be an **Exchange Administrator** with the **Permissions Admin** role for the **Recipients** configuration level:

- The Windows user account that is specified as the `NetIQmc` service account on the managed Exchange server.
- The Windows account of the user who is running the main AppManager setup program.

If you do not want the agent to create the mailbox, you can manually create the mailbox. For more information, see "Configuring Exchange Server Mailbox and Profile Information in Security Manager" on page 11.

Chapter 3
Installing AppManager for Microsoft Exchange 2000 or 2003

This chapter provides installation instructions for AppManager for Microsoft Exchange 2000 or 2003.

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.

Installing the Module

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

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

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

- Run the module setup program, `AM70-Exchange2000-7.x.x.0.msi`.
- Use Control Center to install the module on the remote computer where an agent is installed. For more information, see "Deploying the Module with Control Center" on page 11.

To install the module manually:

1. Run the module setup program on all Microsoft Exchange computers you want to monitor. If you are installing the module on an Exchange server that is configured with Exchange Virtual 2000 or 2003 Servers, select **Launch Configuration utility**. For more information, see "Configuring User Account and Mailbox Information for Virtual Servers" on page 12.
2. Run the module installer on all console computers to install the Help and console extensions.
3. To install the Knowledge Scripts and, where relevant, the Analysis Center reports:
   a. When installing to the primary QDB, select **Install Knowledge Scripts**.
   b. ***If Analysis Center reports are available for this module***, select **Install report package**.
   c. Specify the SQL Server name of the server hosting the QDB as well as the case-sensitive QDB name.

d. ***If Analysis Center reports are available for this module***, specify the SQL Server name of the server hosting the Analysis Center Configuration Database.

Notes

- You can install the Knowledge Scripts and Analysis Center reports to local or remote databases.
- You need to install these module components only once per database.

4. ***If you use Control Center 7.x***, run the module installer for each QDB attached to Control Center.
5. ***If you use Control Center 8.x***, run the module installer only for the primary QDB, and Control Center will automatically replicate this module to secondary QDBs.
6. ***If you have repositories running in active/active or active/passive clusters***, run the module installer on the active node. Then, copy the following Registry key to the non-active node.

   `HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\AppManager\4.0`

7. *If the module setup program is unable to connect with the management server*, you must manually update the AppManager repository with the Exchange server profile and mailbox information. For more information, see "Configuring Exchange Server Mailbox and Profile Information in Security Manager" on page 11.
8. *If you have not already discovered Microsoft Exchange 2000 or 2003 resources*, run the Discovery_Exchange Knowledge Script on all agent computers where you installed the module. For more information, see "Discovering Exchange Server Resources" on page 14.

   AppManager for Microsoft Exchange 2000 or 2003 supports discovering and monitoring Windows clusters *only* in AppManager version 7.x or later.
9. *To discover an EVS in a cluster environment*, run the Discovery_Cluster Knowledge Script on the physical node that owns the cluster. You must create new jobs and reports on EVS objects and delete existing jobs if they are already running on the physical node. For more information, see "Configuring and Monitoring Clusters" on page 25.
10. Upgrade running jobs for any Knowledge Script changes. For more information, see "Upgrading Knowledge Script Jobs" on page 15.

After installation has completed, the `Exchange2000_Install.log` file, located in the `\NetIQ\Temp\NetIQ_Debug\<ServerName>` folder, lists any problems that occurred.

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.

Deployment Overview

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

To deploy the module on an agent computer:

1. Verify the default deployment credentials.
2. Check in an installation package.
3. Configure an 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.

Checking In the Installation Package

You must check in the installation package, `AM70-Exchange2000-7.x.x.0.xml`, before you can deploy the module on an agent computer.

To check in a module installation package:

1. Log on to Control Center and navigate to the Administration view.
2. In the Deployment folder, select **Packages**.
3. On the Tasks pane, click **Check in Packages**.
4. Navigate to the folder where you saved `AM70-Exchange2000-7.x.x.0.xml` and select the file.
5. Click **Open**. The Deployment Package Check in Status dialog box displays the status of the package check in.

Configuring Exchange Server Mailbox and Profile Information in Security Manager

If the setup program is unable to connect with the management server during agent installation, you must manually update the AppManager repository with the Exchange server profile and mailbox information.

AppManager for Exchange 2000 or 2003 uses Exchange server profile and mailbox information to run Exchange Knowledge Scripts. The Exchange Knowledge Scripts in turn require profile and mailbox information on a group of Exchange servers. For example, to monitor connectivity between a group of Exchange servers, the MAPI mail profile name that AppManager associates with the monitoring service Log On As account and mailbox information for each server must be in the repository. AppManager uses this sensitive information to send and receive test mail messages.

The following Knowledge Scripts require Exchange profile and mailbox alias information. You must update the profile and mailbox alias information in the AppManager repository for each Exchange server you want to monitor with these Knowledge Scripts:

Connectivity	PFAclInfo
InactiveMailboxes	PFInfo
InactivePublicFolders	PFReplicationByObj
MailboxesOverStorageLimit	ResponseTime
MailboxesWithoutStorageLimit	SMTPConnectivity
NumberofMailboxes	TopNISMailboxRes
PFAclChanges	TopNISPublicRes

Complete the following fields on the Exchange 2000/2003 tab in AppManager Security Manager:

Field	Description
Server Name	Name of the Exchange server or virtual server
Profile	Exchange profile name created by the AppManager setup program
Mailbox Alias	Exchange mailbox alias name.

Configuring User Account and Mailbox Information for Virtual Servers

If you are installing the module on an Exchange server that is configured with Exchange virtual servers, a separate instance of the monitoring service is installed for each virtual server, and you are prompted for account and mailbox information for each instance of the service.

To use the AppManager setup program to create a new user and mailbox:

1. In the final dialog box of the AppManager for Microsoft Exchange 2000 or 2003 installation procedure, select **Launch configuration utility** and then click **Finish**.
2. In the AppManager for Microsoft Exchange 2000 or 2003 Server Configuration dialog box, complete the following fields for each server:

Field	Description
Exchange Information for server	Specify the name of the Microsoft Exchange server you want to configure.
Mail Box Name	Specify the name of the mail box applicable for the Microsoft Exchange server.
Profile Name	Specify the profile name applicable for the Microsoft Exchange server.
Domain	Specify the domain where the Microsoft Exchange server is installed.
Username	Specify the username applicable for connecting to an instance of the Microsoft Exchange server.
Password	Specify the password applicable for the username.

3. Click **Next**.
4. Verify that the configuration summary details are valid and then click **Finish**.

Running the Setup Program on a Windows Vista Console Computer

If you are using Microsoft Vista on your Operator Console or Control Center Console computer, you must run `AM70-Exchange2000-7.x.xx.0.msi` using the "Run as administrator" option from the Vista command prompt menu.

To run the setup program on Windows Vista:

1. From the Vista Start menu on the console computer, click **All Programs**, and then click **Accessories**.
2. Right-click **Command Prompt** and select **Run as administrator**.
3. In the command prompt window, navigate to the location of the module setup program.
4. At the prompt, type `AM70-Exchange2000-7.x.xx.0.msi` and press `[Enter]`.
5. Continue the module setup process from step 5 in "Installing the Module" on page 9.

Silently Installing the Module

To silently (without user intervention) install a module, create an initialization file (`.ini`) for this module that includes the required property names and values to use during the installation.

To create and use an initialization file for a silent installation:

1. Create a new text file and change the filename extension from `.txt` to `.ini`.
2. To enable AppManager to automatically start the Exchange Directory service, include the following text in the `.ini` file:

   ```
   MO_STARTEXCH=true
   ```

3. Save and close the `.ini` file.
4. Run the following command from the folder in which you saved the module installer:

   ```
   msiexec.exe /i "AM70-Exchange2000-7.x.x.0.msi" /qn MO_CONFIGOUTINI="full path
   to the initialization file"
   ```

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

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

```
/L* "AM70-Exchange2000-7.x.x.0.msi.log"
```

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

Discovering Exchange Server Resources

Use the Discovery_Exchange Knowledge Script to discover Microsoft Exchange 2000 or 2003 configuration and resources.

In Exchange Server 2003, if you change the location of the Exchange tracking logs through the Exchange System Manager, you must re-run this script to discover the new log path.

To discover and monitor Microsoft Exchange 2000 Server or Exchange Server 2003, you must delegate Exchange View Only Administrator permission to the monitoring service Log On As account. The AppManager setup program does not delegate permission to the monitoring service Log On As account.

Set the parameters on the Values tab as needed:

Description	How to Set It
Raise event when discovery succeeds?	This Knowledge Script raises an event when the job fails for any reason. In addition, you can set this parameter to y to raise an event when the job succeeds. The default is n.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25 (blue event indicator).
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5 (red event indicator).
Event severity when discovery is partially done	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery returns some data but also generates warning messages. The default is 10 (red event indicator).
Event severity when discovery is not applicable	Set the event severity level, from 1 to 40, to reflect the importance of an event in which the target computer does not have Exchange Server installed. The default is 15 (yellow event indicator).

Troubleshooting the Installation

Installation-related problems reported by AppManager for Microsoft Exchange 2000 or 2003 users include the following:

- Exchange 2000 or Server 2003 is not installed on the target computer.
- The module installation program attempts to create a mailbox that already exists on the Exchange server.
- The AppManager management server and repository have not been installed successfully, or there are network communication problems.

If you install the AppManager repository and AppManager management server before installing the AppManager agent and there are no network communication problems, details about each managed client are automatically discovered and added to the Operator Console. If installation or discovery fails, check the Operator Console for information about the failure.

If you do not see the Exchange view or the configuration details for the target Exchange server, perform the following actions:

- Ensure the AppManager agent services, `NetIQmc` and `NetIQccm`, are installed and running on the target server. To view the target Microsoft Exchange 2000 or Microsoft Exchange Server 2003 in the Computer List, use the **Services** Control Panel or run the **NT_RemoteServiceDown** Knowledge Script on the management server.
- Ensure you ran the configuration utility when installing AppManager for Microsoft Exchange 2000 or 2003 on an Exchange server configured with virtual servers. The configuration utility allows you to create a user account and mailbox. For more information, see "Configuring User Account and Mailbox Information for Virtual Servers" on page 12.
- Manually run the Discovery_Exchange Knowledge Script from the Operator Console. For more information, see "Discovering Exchange Server Resources" on page 14.

Upgrading Knowledge Script Jobs

This release of AppManager for Microsoft Exchange 2000 or 2003 may contain updated Knowledge Scripts. 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.

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 Web 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.

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. Customized script parameters may have reverted to default parameters during the installation of the module. New parameters may need to be set appropriately for your environment or application.

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 both 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. Click **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.

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 16.

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. On the KS menu, select **Properties propagation > Ad Hoc Jobs**.
3. ***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, including the schedule, actions, and Advanced properties.

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.

Chapter 4
Developing a Monitoring Strategy

AppManager for Microsoft Exchange 2000 or 2003 provides a variety of Knowledge Scripts to monitor Exchange 2000 or Server 2003, related services such as Active Directory and IIS, as well as server components such as memory, CPU and disk space. To determine how you are going to use these Knowledge Scripts, it is useful to have an overview of the Exchange components you plan to monitor using AppManager. This chapter also lists the Knowledge Scripts that you can use to monitor your Exchange environment.

Understanding Which Exchange Server Components to Monitor

Monitoring all the components of an Exchange environment can seem a daunting task. However, if you define specific server functions and identify the Knowledge Scripts that monitor those functions, you can build your strategy around that framework.

You can use any combination of Knowledge Scripts to monitor the servers, collect data, and initiate responsive and corrective actions. All the Knowledge Scripts in the Exchange and Exchange2000 categories monitor both Exchange 2000 and Exchange Server 2003 environments.

To effectively monitor Exchange, you need to determine which Knowledge Scripts to run on an ongoing basis. For example, connectivity and response time are critical in most environments and should be monitored frequently, while POP3 server activity can range from constantly high to almost nothing, depending on the number of remote users.

AppManager for Microsoft Exchange 2000 or 2003 provides tools to monitor the following features of Exchange:

- Connectivity and response time
- Databases and log files
- Server performance and workload
- Protocols and virtual servers
- Services
- Connectors
- Message queues
- Outlook Web Access

Monitoring Connectivity and Response Time

NetIQ Corporation recommends that you also install and run AppManager ResponseTime for Exchange, an AppManager module that performs synthetic user transactions on an Exchange server, such as:

- Sending and receiving an e-mail message
- Tracking server connectivity
- Measuring server response time

AppManager for Microsoft Exchange 2000 or 2003 allows you to test and monitor connectivity in the following scenarios:

- From one server to another, from one server to multiple others, and among many servers
- Between your Exchange servers and specified Internet domains

AppManager for Microsoft Exchange 2000 or 2003 allows you to test and monitor response time in the following scenarios:

- Measure how long it takes a "sending" server to receive a confirmation reply from a "receiving" server
- On a single server that tests the client-server components on that computer, and among multiple servers that tests the client-server components on all included computers

With an overview of connectivity and response time, you can make a strategy to monitor the following activities:

- End-to-end connectivity between one Exchange server and one or more other servers
- End-to-end connectivity among all Exchange servers in your organization
- Connectivity between your Exchange servers and specified Internet domains
- Response time for each Exchange server connection in your organization

Use the following Knowledge Scripts to monitor Exchange connectivity and response time:

- Connectivity
- ResponseTime
- SMTPConnectivity
- SMTPConnectivityEx

Monitoring Databases and Log Files

Exchange 2000 and Server 2003 rely on a number of databases that are collectively known as the information store. The information store contains the following types of databases:

- The mailbox store - contains user mailboxes
- The public folder store - contains public folders

Exchange supports multiple mailbox and public folder stores. Storage groups contain mailbox stores and public folder stores. Each storage group has a transaction log file associated with it. The transaction log file is a record of every set of changes made to the databases in a storage group.

With an overview of Exchange databases and log files, you can make a strategy to monitor the following:

- The size of the mailbox store
- The size of the public folder store

- The size of the Exchange databases
- The wasted space within those databases that are inactive for prolonged periods and can be removed
- The size of the transaction log associated with each storage group.

Note
By default, transaction logs are not deleted until a full backup of the storage group is performed. If there is a high volume of traffic to and from your Exchange databases or the backup of the storage group is delayed for some reason, the transaction logs can use significant disk space.

- The database activities such as the following:
  - The number of connections to the databases for a given period of time
  - The number of requests per second to open folders in the mailbox and public folder stores
  - The delivery times for messages submitted to each store (the time from when the message was submitted to when it was delivered)
- The number of connections and requests to open folders
- The message delivery time
- The databases for which mailboxes and public folders use the most disk space
- The users who are sending and receiving the most e-mails
- The access control lists for public folders to help implement security
- The public folder object replication to ensure that your Exchange servers replicate information properly in public folders
- The mount and dismount status of each mailbox and public folder store.

Use the following Knowledge Scripts to monitor the mailbox and public folder stores, and the associated transaction log files:

- ISMailboxStoreSize
- ISPubStoreSize
- MailboxesOverStorageLimit
- MailboxesWithoutStorageLimit
- NumberOfMailboxes
- PFInfo
- InactiveMailboxes
- InactivePublicFolders
- ISLogFileSize
- ISConnections
- ISMailboxStoreOpens
- ISPubStoreOpens
- ISMailboxStoreAvgDlvryTime
- ISPubStoreAvgDeliveryTime
- TopNISMailboxRes
- TopNISPublicRes
- TopNReceivers
- TopNSenders
- DynSecsOldestMsgInMTAQueue
- PFAclInfo
- PFReplicationByObj
- NumberOfMailboxes
- PublicStoreMountStatus

Monitoring Server Performance and Workload

Although it is useful to monitor individual components of Exchange 2000 or Server 2003, you can also gain insight from monitoring the overall performance and workload of the servers.

To understand how effectively your hardware configurations are supporting your implementation of Exchange 2000 or Server 2003, you can monitor processor and memory performance. AppManager for Microsoft Exchange 2000 or 2003 allows you to gather information about the following:

- The amount of time the processors on your Exchange servers are busy
- The percentage of time the Exchange process threads are executing instructions
- The amount of paging activity

An application may use all of the available processing power from time to time. However, if Exchange is routinely using the maximum available processing power for extended periods, it is likely that you have underestimated the workload of your system. The same holds true for memory use. If you observe an unusual amount of paging activity on your Exchange servers, it may mean that there is insufficient physical memory.

In maintaining your Exchange environment, you need an overall picture of the workload carried by your servers. The workload can be more clearly understood when you have data for the total number of messages handled by your servers, the rate at which servers send and receive messages, the extent to which messages are queued before being processed, and the number of users connecting to your servers.

With an overview of Exchange server performance and workload, you can develop a strategy to monitor the following:

- The extent to which Exchange uses available processing power and memory
- The total number of messages handled by your servers
- The rate at which the servers send and receive messages
- The number of messages held in the various queues
- The number of users connecting to your Exchange servers

Use the following Knowledge Scripts to monitor Exchange server performance and workload:

- ServerHealth
- ServerHistory
- ServerLoad
- ServerQueues
- ServerTotalMsg
- ServerUsers

Monitoring Protocols and Virtual Servers

Exchange 2000 and Server 2003 use a number of protocols to support communication between remote clients and the information store. Each protocol object provides a virtual server for the remote clients using that protocol.

The POP3 and IMAP4 protocols provide Internet access to your Exchange servers. Internet access allows users who cannot maintain permanent connections to your Exchange servers to access their e-mail. POP3 provides access only to a user's mailbox, while IMAP4 allows a user to access public folders, as well. The NNTP protocol implemented by Exchange 2000 and Server 2003 allows Outlook users to take part in Internet discussion groups, and allows NNTP client applications to access news group public folders on an Exchange server.

With an overview of the protocols and virtual servers supported by your Exchange servers, you can develop a strategy to monitor the following:

- The authentications performed by the POP3 and IMAP4 protocols
- The current and total number of connections to each virtual server

- The number of access operations performed by each virtual server
- The total, outbound, current, and SSL connections to the NNTP virtual server
- The up and down status of the HTTP, IMAP4, NNTP, POP3, and SMTP virtual servers and optionally restart a server that is down
- The failure rate for authentications made by the IMAP4 and POP3 protocols
- The total number of authentications and the rate of authentications
- The number of connections to the virtual servers and the number of access operations performed by the virtual servers. This will help you determine whether you have properly limited the number of connections to the server, how quickly idle connections are terminated, and whether your hardware configuration is adequate to the number of connections.
- The connections to the NNTP virtual server
- The up and down status of virtual servers to ensure the availability of those servers. If a server is detected down, AppManager attempts to restart it, and raises an event to inform you that the server was down.

Use the following Knowledge Scripts to monitor the virtual servers Exchange uses for each Internet protocol:

- IMAP4Accesses
- IMAP4Authenticate
- IMAP4Connections
- POP3Accesses
- POP3Authenticate
- POP3Connections
- NNTPConnections
- ProtocolVSStatus

Monitoring Services

Exchange 2000 and Server 2003 use the following services to implement messaging:

- **Site Replication service**: This service replicates directory information in environments where you use both Exchange 2000 and Server 2003.
- **Information Store service**: This service manages the mailbox and public folder stores.
- **MTA Stacks service**: This service connects Exchange to other messaging systems.

You need to monitor any Exchange service running on one of your servers. When you run the Discovery_Exchange Knowledge Script on an Exchange server, AppManager for Microsoft Exchange 2000 or 2003 adds a **Services** object to the TreeView as a child of that Exchange server. The **Services** object lists all the Exchange services running on that computer.

After you discover Exchange services, you can monitor these services for the up and down status and restart any service.

Use the following Knowledge Scripts to monitor Exchange services:

- SRSServiceDown
- ServicesDown

Monitoring Connectors

Exchange 2000 and Server 2003 use connectors to transfer messages between the following entities:

- Routing groups
- Servers running different versions of Exchange
- Exchange and other mail systems

Connectors also synchronize directory information between Exchange and other mail systems.

Exchange uses the following connectors to facilitate communication between routing groups:

- Routing Group connector
- SMTP connector
- X.400 connector

You can configure multiple connectors between routing groups to facilitate load balancing and fault tolerance.

To enable Exchange users to communicate with users of other messaging systems, Exchange uses the following connectors:

- Lotus Notes connector
- Lotus cc:Mail connector
- Novell GroupWise connector
- Microsoft Mail connector
- Schedule+ Free/Busy connector

Use the ConnectorStatus Knowledge Script to monitor the up/down status of Exchange connectors and to raise an event if a specified connector is detected as down.

Monitoring Message Queues

Electronic messages wait in a number of queues before reaching their destination. All messages in a queue have a common next-destination server. A queue that contains messages with a common next-destination server is known as a link queue. A queue that contains messages with a common final-destination server is called a destination queue.

The SMTP protocol (through its virtual server) is responsible for sending emails from one Exchange server to another, and from one email system to another.

Exchange servers use the X.400 protocol (through its virtual server) to connect routing groups within Exchange, and to route messages to other X.400 systems.

With an overview of the types of message queues in an Exchange server, you can develop a strategy to monitor:

- SMTP inbound, outbound, and link queues for total messages, size in bytes, and length of time messages stay in queues
- X.400 inbound, outbound, and link queues for total messages, size in bytes, and length of time messages stay in queues

By monitoring these message queues, you can determine how effectively Exchange is handling the transfer of messages. The Exchange servers hold messages in queues while routing tasks such as content conversion and address resolution are performed. For example, if you find that a queue holds an inordinate number of messages, or that messages remain in a queue for extended periods, it means that the basic routing functions of Exchange have failed.

Use the following Knowledge Scripts to monitor Exchange message queues:

- DynSecsOldestMsgInMTAQueue
- LinkStatus
- QueueStatus
- MTAConnectionQueueLength
- ServerQueues

Monitoring Outlook Web Access

Outlook Web Access (OWA) provides a Web browser interface to Exchange 2000 or Server 2003, allowing users remote access to e-mail, calendars, group scheduling, and collaboration applications. OWA connects to Exchange through the HTTP virtual server.

AppManager for Microsoft Exchange 2000 or 2003 provides Knowledge Scripts to monitor the number of messages sent from OWA, and the number of messages opened from OWA.

An Exchange virtual server can accept as many incoming connections as the system resources can handle. By monitoring OWA activity, you can gauge the demands placed on a computer hosting the HTTP virtual server. You can control the demands placed on that computer by limiting the number of connections the HTTP virtual server will accept, or by dedicating a separate front-end server to handle those connections.

With an overview of how OWA connects to your Exchange environment, you can make a strategy to monitor:

- The number of messages sent from OWA
- The number of messages opened from OWA

Use the following Knowledge Scripts to monitor OWA activity:

- MsgsOpenedByOWA
- MsgsSentByOWA

Monitoring Windows 2000 Services

Exchange 2000 or Server 2003 is closely integrated with the Windows 2000 operating system. AppManager for Microsoft Exchange 2000 or 2003 provides broad monitoring capabilities for:

- Active Directory services
- Internet Information Services (IIS)

AppManager for Microsoft Exchange 2000 or 2003 allows you to monitor the following:

- The health and availability of Active Directory domain controllers
- The availability of the Global Catalog
- The use of physical resources by IIS
- The extent to which the servers utilize the Internet protocols

Monitoring Overall Server Performance

In addition to monitoring Exchange 2000 or Server 2003-specific activity, AppManager for Microsoft Exchange 2000 or 2003 provides Knowledge Scripts for monitoring other related aspects of server performance, such as the following:

- The overall memory and CPU usage by your servers
- The physical and logical disks
- The specific system ports

By developing a comprehensive strategy to monitor Exchange components and the general health of your servers, you can ensure an effective implementation of Exchange 2000 or Server 2003.

Chapter 5
Configuring and Monitoring Clusters

Clustered groups are a feature of Windows 2000 Server and Windows Server 2003. You can install Exchange 2000 or Server 2003 on the nodes of a clustered group and have the advantages of clustering available to your messaging environment. There are two types of Windows clustering:

- Active/Passive
- Active/Active

AppManager for Microsoft Exchange 2000 and 2003 supports monitoring Windows clusters *only* in AppManager version 7.x. For more information about clusters, see the *AppManager for Microsoft Cluster Server Management Guide*.

Adding an Exchange Server Cluster to the TreeView

Add the individual nodes of a cluster to the Operator Console TreeView pane, and then group them accordingly.

For example, if `EX2KSVR_1` and `EX2KSVR_2` are the two nodes of a Microsoft Exchange Server 2000 or Microsoft Exchange Server 2003 cluster, add each of these computers to the TreeView.

After the computers are visible in the TreeView pane, create a server group, for example, `EX2K_CLUSTER_1`, and add each computer to that group.

For more information about adding computers to the TreeView and creating server groups, see the *Operator Console User Guide for AppManager*.

Discovering EVS and Nodes

To discover an EVS in a cluster environment, run the Discovery_Cluster Knowledge Script, which allows you to add the cluster resource objects or work on the cluster nodes. You can directly work with the cluster objects to avoid the Active/Passive state from failover or offline nodes.

Discovering Resources on Cluster Nodes

To discover resources on an Exchange 2000 or Server 2003 cluster, run the following Discovery Knowledge Scripts in the order listed:

Knowledge Script	Resources Discovered
Discovery_NT	Windows 2000 configuration and resources (for example, memory, physical and logical disks, and CPU).
Discovery_MSCS	Microsoft Cluster Service configuration and resources (for example, cluster services, and nodes in a cluster).
Discovery_Cluster	Exchange Virtual Server objects
Discovery_Exchange	Exchange 2000 or Server 2003 configuration and resources, such as Exchange services, storage groups, and protocols. When you discover Exchange resources, AppManager for Microsoft Exchange 2000 or 2003 lists each EVS that a computer can own as a child object of that computer, regardless of whether the EVS is active at the time of discovery.

For information about monitoring cluster resources, see "Monitoring Resources on Cluster Nodes" on page 26.

Discovering Resources on the EVS

To discover resources on an Exchange 2000 or Server 2003 Virtual Server, run the Discovery_Exchange Knowledge Script, which discovers Exchange configuration and resources such as services, storage groups, protocols, and each EVS and the underlying physical nodes. For more information, see "Discovering Exchange Server Resources" on page 14.

Monitoring Resources on Cluster Nodes

You should monitor the resources on each node of the cluster. For example, to monitor memory usage, run the NT_MemUtil Knowledge Script on each node of the cluster. To monitor CPU usage, run the NT_CpuLoaded Knowledge Script on each node of the cluster.

Monitoring resources on cluster nodes varies from the standard practice in monitoring an Exchange Virtual Server and its resources. For example, when monitoring EVS 1 on Node 1, you want to continue monitoring if Node 1 fails and EVS 1 is moved to Node 2. To monitor a Virtual Server as it moves from node to node, use the Cluster-Aware Knowledge Scripts. For more information, see "Running Cluster-Aware Knowledge Scripts" on page 27.

Running Cluster-Aware Knowledge Scripts

To monitor a virtual server as it moves from node to node, run the cluster-aware Knowledge Scripts on each instance of the server. The following Knowledge Scripts are cluster aware:

Exchange tab	Exchange2000 tab
Connectivity	ISPubStoreOpens
InactiveMailboxes	ISPubStoreSize
ISLogFileSize	LinkStatus
MailboxesOverStorageLimit	MsgAvgLocalDlvryTimeByIntrv
MailboxesWithoutStorageLimit	MsgsAvgLocalDeliveryTime
MsgsByServer	MsgsBetweenAdminGroups
ServerHealth	MsgsBtwnAdmnGrpsByInterval
ServerHistory	MsgsOpenedByOWA
ServerLoad	MsgsSentByOWA
ServerQueues	MsgsThroughSMTPService
ServerTotalMsg	MsgsThruSMTPSvcByInterval
ServerUsers	MsgsWithinAdminGroup
SMTPConnectivity	MsgsWthnAdmnGrpByInterval
TopNISMailboxRes	MTAConnectionQueueLength
TopNReceivers	POP3Accesses
TopNSenders	POP3Authenticate
DynSecsOldestMsgInMTAQueue	POP3Connections
MsgsByServerByInterval	ProtocolVSStatus
MsgsBySize	QueueStatus
MsgsOfSystem	CategorizerHealth
MsgsSpecificDomain	CategorizerMessages
MsgsSpecificDomainByInterval	IMAP4Accesses
MsgsThroughConnector	IMAP4Authenticate
NumberOfMailboxes	IMAP4Connections
ResponseTime	ISConnections
SMTPConnectivityEx	ISMailboxStoreAvgDlvryTime
ISMailboxStoreOpens	ConnectorStatus
ISMailboxStoreSize	ISPubStoreAvgDeliveryTime

Collecting Data

Although you are monitoring virtual servers, AppManager for Microsoft Exchange 2000 or 2003 associates the collected data with the physical node.

When you run a job on an EVS, the job collects data for that EVS and the physical node where the EVS is online. To avoid data collection from the physical node, change the data collection settings in the Preferences tab.

When you run a job on the physical node, the job collects data for the EVSs that are online on that particular physical node.

For example:

1. **Node cluster with Active/Active configuration**

   If EVS1 is active on EX2KSVR_1 and EVS2 is active on E2KSVR_2, when you run a job on EVS1, the job creates two data streams:

   - Data stream for EVS1
   - Data stream for E2KSVR_1

   When you run a job on E2KSVR_1, the job collects data for EVS1. When EVS2 fails over to E2KSVR_1 and when you run a job on E2KSVR_1, the job creates two data streams:

   - Data stream for EVS1
   - Data stream for EVS2

2. **Node cluster with Active/Passive configuration**

   If EVS1 is active on EX2KSVR_1, when you run a job on EVS1, the job creates two data streams:

   - Data stream for EVS1
   - Data stream for E2KSVR_1

   When EVS1 is failed over to E2KSVR_2, the job creates two data streams:

   - Data stream for EVS1
   - Data stream for E2KSVR_2

Understanding False Data Due to MAPI Limitations

AppManager for Microsoft Exchange 2000 or 2003 uses MAPI to test the messaging system by pushing email messages between physical nodes and measuring the latency. The servers return false data if a MAPI-based script pushes email messages between virtual servers on the same physical node.

For example, the Exchange_Connectivity and Exchange_ResponseTime Knowledge Scripts expose a limitation of MAPI where AppManager for Microsoft Exchange 2000 or 2003 cannot measure the latency between virtual servers running on the same physical node. These scripts collect data accurately when AppManager for Microsoft Exchange 2000 or 2003 measures latency between physical nodes. However, if a failover occurs and the monitored virtual servers begin running on the same node, then the scripts continue to run but the collected data indicates that the email message is not moving between the virtual servers. Assuming normal operation of the virtual servers, email messages continue between the virtual servers, but the current implementation of MAPI does not expose this limitation.

To work around this problem, monitor virtual servers from an Exchange server outside the cluster.

Sample Cluster Configurations

The following examples are provided to help you identify the resources required to install AppManager for Microsoft Exchange 2000 or 2003 on a cluster.

Example 1: Two Nodes with Two Exchange Virtual Servers

Exchange Virtual Server Name	Log On As Account	Mailbox Name	Profile Name	Drive Letter	NetIQ Monitoring Service
PPFTXExchMA	PPFTXExchMA	PPFTXExchMA	PPFTXExchMA	T:	Qexch2ka1
PPFTXExchMB	PPFTXExchMB	PPFTXExchMB	PPFTXExchMB	U:	Qexch2ka2
Computer Names: PPFtxnode1 and PPFtxnode2.					
Cluster Failover Notes: Active/Active cluster.					

Example 2: Two Nodes with Two Exchange Virtual Servers

Exchange Virtual Server Name	Log On As Account	Mailbox Name	Profile Name	Drive Letter	NetIQ Monitoring Service
MammaExchMA101	MammaExchMA101	MammaExchMA101	MA101	T:, S:	Qexch2ka1
MammaExchMA102	MammaExchMA101	MammaExchMA101	MA101	U:, V:	Qexch2ka2
Computer Names: Mammanode1 and Mammanode2.					
Cluster Failover Notes: Active/Active cluster.					

Example 3: Three Nodes with Two Exchange Virtual Servers

Exchange Virtual Server Name	Log On As Account	Mailbox Name	Profile Name	Drive Letter	NetIQ Monitoring Service
CHVExchMA	CHVExchMA	CHVExchMA	MA	T:, S:	Qexch2ka1
CHVExchMB	CHVExchMB	CHVExchMB	MB	U:, V:	Qexch2ka2
Computer Names: CHVnode1, CHVnode2, and CHVnode3.					
Cluster Failover Notes: A passive node can accept only ONE virtual server. It is not possible for one node to have more than one virtual server on it at a time.					

Example 4: Five Nodes with Four Exchange Virtual Servers

Exchange Virtual Server Name	Log On As Account	Mailbox Name	Profile Name	Drive Letter	NetIQ Monitoring Service
PUBExchSingA	PUBExchSingA	PUBExchSingA	SingaporeVSa	R:	Qexch2ka1
PUBExchSingB	PUBExchSingB	PUBExchSingB	SingaporeVSb	S:	Qexch2ka2
PUBExchSingC	PUBExchSingC	PUBExchSingC	SingaporeVSc	T:	Qexch2ka3
PUBExchSingD	PUBExchSingD	PUBExchSingD	SingaporeVSd	U:	Qexch2ka4
Computer Names: PUBnode1, PUBnode2, PUBnode3, PUBnode4, and PUBnode5.					

Exchange Virtual Server Name	Log On As Account	Mailbox Name	Profile Name	Drive Letter	NetIQ Monitoring Service
Cluster Failover Notes: A passive node can accept only ONE virtual server. It is not possible for one node to have more than one virtual server on it at a time.					

Example 5: Six Nodes with Four Exchange Virtual Servers

Exchange Virtual Server Name	Log On As Account	Mailbox Name	Profile Name	Drive Letter	NetIQ Monitoring Service
PUBExchSingA	PUBExchSingA	PUBExchSingA	SingaporeVSa	R:	Qexch2ka1
PUBExchSingB	PUBExchSingB	PUBExchSingB	SingaporeVSb	S:	Qexch2ka2
PUBExchSingC	PUBExchSingC	PUBExchSingC	SingaporeVSc	T:	Qexch2ka3
PUBExchSingD	PUBExchSingD	PUBExchSingD	SingaporeVSd	U:	Qexch2ka4
Computer Names: PUBnode1, PUBnode2, PUBnode3, PUBnode4, PUBnode5, and PUBnode6.					
Cluster Failover Notes: Only PUBnode5 and PUBnode6 are passive nodes. PUBnode1, 2, 3, and 4 can only host their assigned Exchange Virtual Server.					

Chapter 6
Maintaining the Environment

AppManager for Microsoft Exchange 2000 or 2003 enables you to perform periodic and occasional maintenance tasks when managing your Exchange 2000 or Server 2003 environment.

Scheduling Maintenance Periods

Administrators periodically take Exchange 2000 or Server 2003 servers and databases off-line to perform necessary maintenance on the servers and to backup or repair databases. During times when these resources are unavailable, your AppManager for Microsoft Exchange 2000 or 2003 monitoring jobs can raise unnecessary events or fail to run. For example, if you shut down a server, any Exchange_Connectivity job in which that server is named raises unnecessary events.

If you take a mailbox store off-line, a job that depends on one of those mailboxes fails. For example, the `qexch2k1a` service logs on with an account that has a mailbox and alias; if the `qexch2k1a` service attempts to send email from a mailbox that is off-line, that job fails.

In addition, jobs fail when you do not stop from the Operator Console before you shut down the Exchange server on which they are running. You can restart each of those jobs from the Operator Console after the Exchange server is on-line.

Blocking Exchange Jobs Temporarily

To avoid the problems of unnecessary events and failed jobs, you can use the AMAdmin_SchedMaint Knowledge Script to:

- Specify the maintenance periods for your Exchange servers
- Prevent Exchange and Exchange2000 Knowledge Script jobs from running on those servers during maintenance periods

Changing a Mailbox Alias

Changing an Exchange mailbox alias prevents AppManager for Microsoft Exchange 2000 or 2003 from recognizing the mailbox and successfully running Knowledge Scripts that rely on that information, such as Connectivity.

If you change the alias, update the information in AppManager Security Manager. For more information about changing the alias information, see the *Administrator Guide for AppManager*.

Deleting Unwanted Emails

Although AppManager for Microsoft Exchange 2000 or 2003 automatically deletes emails used to test connectivity and response time, you should periodically check the mailbox of the account used to send emails and delete any unwanted emails. Periodically deleting unwanted emails ensures the mailbox does not fill up and helps manage disk space on your Exchange server.

To delete unwanted emails:

1. Log on to each Exchange server using the account that is responsible for sending test emails. This account is normally the account used by the `NetIQmc` service on each server.
2. Start Microsoft Outlook.
3. Check the following folders in the left pane of Microsoft Outlook:
   - Deleted Items
   - Inbox
   - Sent Items
4. Delete unwanted emails.

Chapter 7
Exchange and Exchange2000 Knowledge Scripts

The Exchange and Exchange2000 categories provide the following Knowledge Scripts for monitoring Microsoft Exchange 2000 or Server 2003.

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

Knowledge Script	What It Does
CategorizerHealth	Monitors the health of Microsoft Message Categorizer.
CategorizerMessages	Monitors the message traffic of Microsoft Message Categorizer.
ClusterOwner	Determines the node ownership of an Exchange Virtual Server that is part of a cluster.
Connectivity	Monitors mail connectivity between Exchange servers.
ConnectorStatus	Monitors the up/down status of an Exchange connector.
DynSecsOldestMsgInMTAQueue	Reports how long, in seconds, the oldest message has been in the queue of MTA connections.
IMAP4Accesses	Monitors the total number of access operations for the IMAP4 server.
IMAP4Authenticate	Monitors the authentications of IMAP4 protocol stacks.
IMAP4Connections	Monitors the number of current IMAP4 connections and the total number of inbound and outbound connections.
InactiveMailboxes	Monitors the number of mailboxes that have not logged on to the Exchange server for a specified number of days.
InactivePublicFolders	Monitors the number of public folders that have not been accessed or modified for a specified number of days.
ISConnections	Monitors the number of information store connections.
ISLogFileSize	Monitors the size of Exchange log files in the MDBDATA and DSADATA directories on the Exchange server.
ISMailboxStoreAvgDlvryTime	Monitors mailbox store average delivery time to local recipients and storage providers.
ISMailboxStoreOpens	Monitors the rate of requests to the information store to open a mailbox store.
ISMailboxStoreSize	Monitors the disk space used by one or more mailbox stores.

Knowledge Script	What It Does
ISPubStoreAvgDeliveryTime	Monitors public store average delivery time to local recipients and storage providers.
ISPubStoreOpens	Monitors the rate of requests to the information store to open a public store.
ISPubStoreSize	Monitors the disk space used by one or more public stores.
LinkStatus	Monitors the status of all link queues for all X.400 and SMTP virtual servers, including the number, size, and elapsed time that messages reside in a link queue.
LogParser	Parses and queries a specified Exchange log file.
MailboxesOverStorageLimit	Monitors the number of mailboxes over the storage limit.
MailboxesWithoutStorageLimit	Monitors the number of mailboxes with no storage limitations.
MailboxStoreMountStatus	Monitors the mount status of one or more mailbox stores.
MsgAvgLocalDlvryTimeByIntrv	Monitors the average delivery time for local messages since the last time this script ran.
MsgsAvgLocalDeliveryTime	Monitors the average delivery time for local messages for specified days.
MsgsBetweenAdminGroups	Monitors the total number and size of messages transferred between Exchange Admin Groups during the specified number of days or from a specific start date to a specific end date.
MsgsBtwnAdmnGrpsByInterval	Monitors the total number and size of messages sent to an Admin Group or received from an admin group since the last time the Knowledge Script ran.
MsgsByServer	Monitors the number and size of messages transferred between a target Exchange server and all connected servers during the specified number of days or from a specific start date to a specific end date.
MsgsByServerByInterval	Monitors the number and size of messages transferred between a target Exchange server and all connected servers during the monitoring interval.
MsgsBySize	Monitors the number of messages in different size ranges over a specified number of days.
MsgsOfSystem	Monitors the load of directory and public folder replication messages between Exchange sites or Admin Groups.
MsgsOpenedByOWA	Monitors the number of messages opened by Outlook Web Access (OWA).
MsgsSentByOWA	Monitors the number of messages sent by Outlook Web Access (OWA).
MsgsSpecificDomainByInterval	Monitors the total number and size of messages transferred through an Internet Mail Connector (IMC) or SMTP service to and from a specific domain during the monitoring interval (delta value).
MsgsSpecificDomain	Monitors the total number and size of messages transferred through an Internet Mail Connector (IMC) or SMTP service to and from a specific domain during the specified number of days or from a specific start date to a specific end date.
MsgsThroughConnector	Monitors the total number and size of messages sent and received by one or more specified connectors on an Exchange site or routing group.

Knowledge Script	What It Does
MsgsThroughSMTPService	Monitors SMTP messages for the past N days or a range of days.
MsgsThruSMTPSvcByInterval	Monitors SMTP messages since the last time this script ran.
MsgsWithinAdminGroup	Monitors the total number and size of messages transferred between Exchange servers in the same Admin Group during the specified number of days or from a specific start date to a specific end date.
MsgsWthnAdmnGrpByInterval	Monitors the total number and size of messages transferred between Exchange servers in the same Admin Group since last time the Knowledge Script ran (a delta value).
MTAConnectionQueueLength	Monitors the queue length of all message transfer agent (MTA) connections.
NNTPConnections	Monitors connections to the Network News Transfer Protocol (NNTP) service.
NumberOfMailboxes	Monitors the total number of Exchange mailboxes.
PFAclChanges	Checks for changes in the access control lists for each folder in the public information store.
PFAclInfo	Monitors the access control list for each folder in the public information store.
PFInfo	Monitors the number and size of public folders, and the number of messages in the public folders.
PFReplicationByObj	Monitors public folder replication between Exchange servers by updating a test object.
POP3Accesses	Monitors the number of POP3 access operations.
POP3Authenticate	Monitors the authentications of POP3 protocol stacks.
POP3Connections	Monitors the number of current and total connections of POP3 service.
ProtocolVSStatus	Monitors the status of Exchange virtual servers.
PublicStoreMountStatus	Monitors the mount status of one or more public stores.
QueueStatus	Monitors the inbound and outbound message queue status of all X.400 and SMTP virtual servers, including the number, size, and elapsed time that messages reside in a message queue.
Report_Connectivity	Generates a report about the connectivity between Exchange servers.
Report_ISPrivateResourceSummary	Generates a report about the file space used by private information store folders and mailboxes.
Report_ISPublicResourceSummary	Generates a report about the file space used by public information store folders.
Report_ServerLoad	Generates a report about the rate at which messages are being sent and received and the rate at which RPC packets are being processed.
Report_ServerMessage	Generates a report about the total number of mail recipients, messages delivered, messages sent, messages submitted, and messages waiting to be delivered to the mailbox store and the public information stores.
Report_ServerUsers	Generates a report about the number of users connected to the information store.

Knowledge Script	What It Does
Report_TopNMailboxesInfo	Generates a report about the file space (in MB) used by the top private information store folders or mailboxes.
Report_TopNReceivers	Generates a report about which users received the most mail messages, and the total file size of messages received by the top users or by all users.
Report_TopNSenders	Generates a report about which users sent the most mail messages, and the total file size of messages sent by the top users or by all users.
ResponseTime	Checks the mail response time between Exchange servers.
ServerHealth	Monitors the percentage of time that all processors on the Exchange Server are busy and the percentage of elapsed time that the Exchange server process threads are used to execute instructions.
ServerHistory	Monitors the combined message count for the mailbox information and public information stores.
ServerLoad	Monitors the rate at which messages are being received and submitted per minute on the Exchange server.
ServerQueues	Monitors Exchange server queues, including the MTA work queue and the IS Private and the IS Public send and receive queues.
ServerTotalMsg	Monitors the total number of messages for an Exchange server.
ServerUsers	Monitors the number of users connected to the information store.
ServicesDown	Monitors the up and down status of Exchange services.
SMTPConnectivity	Verifies connectivity between an Exchange Server and one or more Internet domains by sending a message to a non-existent account and examining the non-delivery report (NDR).
SMTPConnectivityEx	Verifies connectivity between an Exchange Server and one or more Internet domains by examining the delivery report (DR) or the non-delivery report (NDR).
SRSServiceDown	Monitors the up and down status of the Site Replication Service.
TopNISMailboxRes	Monitors the file space used by the top private information store folders or mailboxes.
TopNISPublicRes	Monitors the file space used by the top public information store folders (public folders).
TopNReceivers	Monitors the total file size of mail messages received by the top users or all users.
TopNSenders	Monitors the total file size of mail messages sent by the top users or all users.

CategorizerHealth

Use this Knowledge Script to monitor the health of Microsoft Message Categorizer, including the rate of:

- Address book lookup completions processed per second
- Address lookups dispatched to Active Directory per second
- Categorization completions per second
- LDAP search completions processed per second
- LDAP searches successfully dispatched per second
- Messages being submitted to the Message Categorizer per second

This script raises an event if a monitored value exceeds the threshold you set.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003 SMTP Virtual Server

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the rate of: • Address book lookup completions processed per second • Address lookups dispatched to Active Directory per second • Categorization completions per second • Lightweight Directory Access Protocol (LDAP) search completions processed per second • LDAP searches successfully dispatched per second • Messages being submitted to the Message Categorizer per second The default is n.
Maximum threshold for the number of address lookup completions processed per second	Specify the maximum number of address lookup completions that can be processed per second before an event is raised. The default is 500.
Maximum threshold for the number of address lookups dispatched to the DS per second	Specify the maximum number of address lookups that can be dispatched to the Directory Service (DS) per second before an event is raised. The default is 500.
Maximum threshold for the rate of categorizations completed	Specify the maximum number of categorizations that can be completed per second before an event is raised. The default is 500.
Maximum threshold for the rate of LDAP search completions processed/sec	Specify the maximum number of LDAP search completions that can be processed per second before an event is raised. The default is 500.

Description	How to Set It
Maximum threshold for the rate of LDAP searches successfully dispatched/sec	Specify the maximum number of LDAP searches that can be successfully dispatched per second before an event is raised. The default is 500.
Maximum threshold for the rate that messages are being submitted to the categorizer	Specify the maximum number of messages per second that can be submitted to the Message Categorizer before an event is raised. The default is 500.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

CategorizerMessages

Use this Knowledge Script to monitor the message traffic of Microsoft Message Categorizer, including the number of messages in the following categories:

- Aborted during the monitoring interval
- Bifurcated during the monitoring interval
- Categorized during the monitoring interval
- Submitted during the monitoring interval
- In the Message Categorizer queue

This script raises an event if the number of messages in a category exceeds the threshold you set.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003 SMTP Virtual Server

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of messages in a category exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of messages: • Aborted during the monitoring interval • Bifurcated during the monitoring interval • Categorized during the monitoring interval • Submitted during the monitoring interval • In the Message Categorizer queue The default is n.
Maximum threshold for the number of messages marked to be aborted by the categorizer	Specify the maximum number of messages that can be marked to be aborted before an event is raised. The default is 200.
Maximum threshold for the number of new messages created by the categorizer (bifurcation)	Specify the maximum number of new messages that can be created by the Message Categorizer (bifurcation) before an event is raised. The default is 200.
Maximum threshold for the number of messages categorizer has submitted to queueing	Specify the maximum number of messages that can be submitted to queueing before an event is raised. The default is 200.
Maximum threshold for the number of messages submitted to the categorizer	Specify the maximum number of messages that can be submitted to the Message Categorizer before an event is raised. The default is 200.

Description	How to Set It
Maximum threshold for the number of messages in the categorizer queue	Specify the maximum number of messages that can be in the Message Categorizer queue before an event is raised. The default is 200.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which the number of messages in a category exceeds the threshold you set. The default is 5 (red event indicator).

ClusterOwner

Use this Knowledge Script to determine whether an Exchange Server computer that is part of a cluster is the owner of the node. This script raises an event if the computer is not the current node owner. In addition, this script generates data streams for ownership status.

Resource Object

Microsoft Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval for this script is Every 5 minutes

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if not node owner? (y/n)	Set to **y** to raise an event if the selected computer is in a cluster but is not the node owner. The default is n.
Collect data for ownership status? (y/n)	Set to **y** to collect data for charts and reports. If enabled, data collection returns the following: • 100 - the computer is a cluster owner or the computer is not in a cluster • 0 - the computer is in a cluster but is not the cluster owner. The default is y.
Event severity when not node owner	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the selected computer is not the node owner. The default is 20.
Raise event when node is down? (y/n)	Set to **y** to raise an event if the selected node is down. The default is y.
Severity when the node is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the elected node is down. The default is 5.
Raise event when EVS is down? (y/n)	Set to **y** to raise an event if the selected EVS is down. The default is y.
Severity when the EVS is down	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the elected EVS is down. The default is 5.

Connectivity

Use this Knowledge Script to monitor mail connectivity between two or more Exchange 2000 or 2003 servers. This script cannot monitor more than one Exchange 2000 or 2003 virtual server.

This script determines whether e-mail can be delivered between Exchange servers and can help you diagnose mail delivery problems, such as problems with network connectivity, Exchange configuration, or Exchange services.

To monitor connectivity for a single Exchange server, use the AppManager ResponseTime for Microsoft Exchange module.

To test complete connectivity between Exchange servers in a non-cluster environment, run this script on the top-level Exchange folder in the Operator Console TreeView. Doing this causes the job to run on all Exchange servers and test each server's connection to the other servers and to itself, verifying complete connectivity between all Exchange servers.

You can also use this script to test connectivity between one server and a list of specified servers. To run this script on a group of Exchange servers, each server must have the same profile name.

If a failover occurs when this script job is running, the job restarts on the new node. It is normal for the job on the failed node to generate one or more error messages, depending on what the job was doing when the failover occurred.

Note

This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information about setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Microsoft Exchange 2000 Server or Exchange Server 2003, Exchange folder

Default Schedule

The default interval is **Every 15 minutes**. This interval is recommended if you are checking connectivity between Exchange servers in a connected network.

If your Exchange servers rely on a remote WAN or LAN service (such as RAS) or a dial-up modem that is not always connected, you can set up server group folders to separate Exchange servers into different groups, then set the schedule interval for this Knowledge Script to run on each folder based on each group's connection schedule.

For example, you can create one server group for your always-connected servers and a separate folder for offhours RAS connections. Further, you can create two sets of jobs with different schedules. The schedules can be frequent for your connected network and once a day for the remote access servers.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a reply to a test message is not received within the specified time interval. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns a value of 100 if the connection between Exchange Servers is up or a value of 0 if the connection is down. The script also returns the response time in seconds for each successful connection between Exchange Servers and the time the connection was attempted. The default is y.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in the AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager. This is especially true if you are running this script as recommended on the top-level Exchange folder or Exchange server groups.
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in the AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager. This is especially true if you are running this script as recommended on the top-level Exchange folder or Exchange server groups.

List of remote servers to monitor	Specify the computer names, separated by commas using the following syntax to check connectivity between specific Exchange 2000 or 2003 servers:
	`<computer>(/O=<organization>/OU=<administrative group>)`
	Where:
	• ***computer*** specifies the name of the computer on which the Exchange server is installed
	• ***organization*** specifies the name of the Exchange organization to which the server belongs
	• ***administrative group*** specifies the name of the Exchange administrative group to which the server belongs
	Separate multiple server names with commas, for example:
	`2K3Server(/O=org/OU=site1),2KServer(/O=Org2/OU=AdminGrp2)`
	This parameter allows you to run this script on a specific Exchange server and check connectivity with other specified servers (1*N). If you leave this field blank, this script checks the connectivity for all servers included in the scope of the job (N*N).

Maximum threshold for a response (in seconds)	Specify the maximum number of seconds that can elapse from the time the test message is sent out until a reply is received. If a reply to the test message is not received within this interval, it is not considered a valid reply. This script raises an event if the threshold is exceeded. The default is 120 seconds.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the response time threshold is exceeded. The default is 5 (red event indicator).

Example of How this Script Is Used

To test connectivity, this script sends a test mail message to each of the Exchange Servers being tested, using the specific account set up for the computer running the job. If the test message is not delivered, the script raises an event to indicate that the server cannot send mail. If the test message delivered by the sending server does not get a reply from each of the receiving servers, the script raises an event indicating the connection with the servers that failed to reply is down. If the test message is delivered but the reply is not received within an acceptable response time, the script raises an event indicating the response time with the server is above the threshold.

Checking Connectivity for Multiple Servers

The AppManager agent uses a mailbox on the local Exchange server where it resides. When you start the script job, the AppManager agent on each server sends a message from its mailbox to each of the other Exchange servers to which you are testing connectivity. Each of the receiving Exchange servers sees the message, and responds back with delivery confirmation.

At the next monitoring interval, the Connectivity job checks to see if the local Exchange server has received mail from the remote servers yet. If a reply has been received, there is connectivity between the local and remote servers. If a reply is not received, the connection is broken and an event is raised.

Assume you have four Exchange servers (a,b,c,d). Each of these servers has a default Exchange client profile and its own unique mailbox. If you run the Connectivity Knowledge Script on these four Exchange servers (a,b,c,d) in the TreeView, the management server starts a job on each of these servers to test connectivity to the other servers and itself, which is essentially a client-to-server connectivity test.

- The job of Exchange server **a** tests connectivity to a,b,c,d
- The job of Exchange server **b** tests connectivity to a,b,c,d
- The job of Exchange server **c** tests connectivity to a,b,c,d
- The job of Exchange server **d** tests connectivity to a,b,c,d

Only Exchange servers on which you run the Connectivity Knowledge Script are included in the connectivity test.

Because connectivity is always tested server to server, it does not matter if the servers are in the same site or different sites. When you create the Connectivity job, you need to include all the servers you want tested in the scope of the job. However, you can use server groups to organize your Exchange servers into sites or use the top level Exchange folder to test connectivity across all sites depending on the range of connectivity testing you want to do. You can also de-select a server you do not want to include in a test using the Objects tab in the Knowledge Script Properties dialog box.

To illustrate these principles, consider an Exchange environment with five Exchange servers: Paris, Cabernet, Dynamo, Boston, and Nero. Each of these servers has a special Windows user account that (1) the `NetIQ Corporationmc` service runs as on that server, and (2) has an Exchange profile and associated mailbox for sending and receiving mail.

If you only run the Connectivity Knowledge Script on the server Paris and do not specify any Exchange servers in the Remote server list, the **netiq-Paris Exchange client** sends a test message from its own mailbox to the **Exchange server Paris** and receives a confirmation when the delivery is successful.

If you run the Connectivity Knowledge Script on the server group, or top level folder that includes Paris and the four other Exchange servers, each server sends a test message to itself and to each of the other Exchange servers in the group. When a delivery confirmation message is received back at each sending server's mailbox within a reasonable period of time, the delivery was successful and connectivity is verified.

An Exchange profile must be associated with a Windows user account such as the `netiq_nt` user account. Although not required for this Knowledge Script, this user should generally be part of the Administrators group if you run other Knowledge Scripts such as ServicesDown to give the user account read, write, and execute permissions on the managed computer.

The Windows user account also needs Exchange Administrator privileges for permission to access to Exchange statistics, an Exchange profile (`netiq-Paris`), and a Mailbox alias (`netiq-Paris`) for sending and receiving mail.

The **mailbox alias** that the agent service `NetIQ Corporationmc` uses should be **unique** for each server. That is, each Exchange Server needs a unique mailbox alias for AppManager to use. Having separate mailboxes that physically reside on each server provides the best coverage for testing connectivity. In addition, using the `netiq-<computer_name>` convention for profiles and mailbox aliases helps you to verify that the test message is delivered to the proper recipients.

During installation, AppManager provides options for automatically creating and configuring profiles and mailbox aliases. If you select this option, the profiles and mailbox aliases are created and checked into the repository for you.

AppManager creates profiles and mailboxes for you even if you do not specify this option, but the information is not stored in the AppManager repository. You can use AppManager Security Manager to add the profile and mailbox names for each Exchange server after installation. You can also use AppManager Security Manager to update the AppManager repository when you change or manually create Exchange profiles and mailboxes.

Checking Connectivity from One Server to a Specified List

In addition to checking complete connectivity, a many-to-many relationship, you can use this Knowledge Script to check connections from a single Exchange server to a specified list of other Exchange servers. For example, assume you have the Exchange server **Paris** at your corporate headquarters. You may only be interested in checking its connectivity to the satellite Exchange servers **Dynamo** and **Cabernet** and not those servers' connectivity to each other.

To do this, you can run this Knowledge Script on Paris and specify `Dynamo,Cabernet` for the `Remote server list` parameter. The job then tests connectivity between Paris and Dynamo and Paris and Cabernet.

Interpreting Response Time Data

If you use this Knowledge Script to collect response time data for graphs and reports, you may notice a saw-tooth pattern of response times.

The peaks and valleys represent the response times found at each interval. The times along the bottom of the graph represent each time the Knowledge Script job ran and collected data.

This saw-tooth pattern is caused by a conflict between the interval set for running this Knowledge Script and a polling mechanism used internally by Exchange Server. Because Exchange is checking and responding internally to the test e-mail message **between job intervals**, the response times returned by the Knowledge Script become skewed.

To avoid this problem, set the interval for this Knowledge Script to some multiple of 56 seconds, for example, 112 and 224 seconds. Using an interval that synchronizes (as much as possible) the Knowledge Script job and the internal mechanism gives you a more consistent and realistic view of the server's response time.

Note

If your primary interest is monitoring the response time between Exchange servers, you may want to use the ResponseTime Knowledge Script rather than the Connectivityowledge Script.

Performing Periodic Maintenance

Periodically log in to each Exchange server using the same Windows account set up for the `NetIQ Corporationmc` service to do some housekeeping. For example, periodically remove old mail messages (that are at least a couple of days old) from the **Inbox,** and permanently remove deleted mail from the **Deleted Item** box. Depending on how frequently you run this script, consider performing these activities weekly or monthly.

ConnectorStatus

Use this Knowledge Script to monitor the status of an Exchange 2000 or 2003 connector. This script raises an event if the connector is detected as down.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a connector is down. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns 100 if the monitored connector is up, 0 if the connector is down. The default is n.
List of connectors to monitor (comma separated)	Specify the names of the connectors you want to monitor, separating multiple names with commas, or specify **ALL** to monitor all connectors on the computer. The default is ALL.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a connector is down. The default is 5 (red event indicator).

DynSecsOldestMsgInMTAQueue

Use this Knowledge Script to identify the ages, in seconds, of messages in MTA queues that exceed a specified threshold.

Resource Object

MTA Queue folder, if dynamically enumerating connections. If you are not enumerating connections dynamically, you can run this script on the MTA Queue folder or on individual queue objects, such as DS Queue, IMC Queue, Public IS Queue, Private IS Queue, Machine Queue, X400 Queue, MSMail Queue, and Directory Queue.

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Create event if old messages are found in a queue?	Set to **Yes** to raise an event if the age of messages in the MTA queue exceeds the threshold you set. The default is Yes.
Severity - Old messages found in queue	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the age of messages in the queue exceeds the threshold. The default is 15 (Yellow event indicator).
Severity - Job failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the DynSecsOldestMsgInMTAQueue job fails. The default is 5 (red event indicator).
Data Collection	
Collect message age data?	Set to **Yes** to collect data for charts and reports. When enabled, data collection returns the age of messages in the queue. The default is unchecked.
Monitoring	
Dynamically enumerate MTA queues	Set to **Yes** to enable dynamic enumeration of MTA queues. The default is Yes.
MTA queue exclude list	If needed, specify a comma-separated list of MTA queues that should not be monitored. For example: `microsoft public mdb,microsoft private mdb`.
Threshold - Age of messages in the queue	Specify the maximum age that messages in the queue can attain before an event is raised. The default is 1440 seconds.

IMAP4Accesses

Use this Knowledge Script to monitor the number of IMAP4 access operations. Access operations include `SELECT`, `EXAMINE`, `APPEND`, `SUBSCRIBE`, `UNSUBSCRIBE`, `LIST` and `SUB` operations. This script raises an event if the total number of IMAP4 access operations exceeds the threshold you specify.

Resource Object

IMAP4 Virtual Server

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of operations exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of IMAP4 access operations. The default is n.
Maximum threshold for number of IMAP4 access operations	Specify the maximum number of IMAP4 access operations that can occur before an event is raised. The default is 10000 access operations.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which the number of operations exceeds the threshold. The default is 5 (red event indicator).

IMAP4Authenticate

Use this Knowledge Script to monitor the authentication of IMAP4 protocols. This script raises an event if the rate of failure of total authentications exceeds the threshold you set.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003, Protocols folder

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of authentication failures exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • Number of authenticate commands received since startup • Number of authenticate commands per second • Number of authenticate command failures since startup The default is n.
Maximum threshold for number of authentication failures	Specify the maximum number of authentication failures that can occur before an event is raised. The default is 1000.
Consecutive number of times before an event	Specify the maximum number of consecutive times the threshold can be exceeded before this script raises an event. The default is 5 consecutive occurrences.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which the number of authentication failures exceeds the threshold. The default is 5 (red event indicator).

IMAP4Connections

Use this Knowledge Script to monitor the number of current IMAP4 connections and the total number of inbound and outbound IMAP4 connections since the IMAP4 service started. This script raises an event if the number of current or total connections exceeds the threshold you set.

Resource Object

IMAP4 Virtual Server

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default option is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • Current connections • Total connections The default option is n.
Maximum threshold for current connections	Specify the maximum number of current IMAP4 connections that can occur before an event is raised. The default is 100 current connections.
Maximum threshold for total connections	Specify the maximum number of IMAP4 connections that can occur before an event is raised. The default is 1000 connections.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

InactiveMailboxes

Use this Knowledge Script to monitor the number of inactive Exchange mailboxes. An inactive mailbox is a mailbox that has not logged on to the Exchange server for a specified number of days. This script raises an event if the number of inactive mailboxes exceeds the threshold you set.

On a computer with more than one virtual server, the total number of inactive mailboxes is calculated as the total number of inactive mailboxes for all virtual servers on the computer.

If a failover occurs when this script job is running, the job restarts on the new node. It is normal for the job on the failed node to generate one or more error messages, depending on what it was doing when the failover occurred.

Note
This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information about setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Microsoft Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of inactive mailboxes exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of inactive mailboxes. The default is n.
Inactive after N days	Specify the number of days to use as a measure of whether a mailbox is inactive. The default is 10 days.
Maximum threshold for number of inactive mailboxes	Specify the maximum number of mailboxes that can be inactive before an event is raised. The default is 300 inactive mailboxes.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.

Description	How to Set It
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of inactive mailboxes exceeds the threshold. The default is 5 (red event indicator).

InactivePublicFolders

Use this Knowledge Script to monitor the number of inactive Exchange public folders. An inactive folder is a public folder that has not been accessed or modified for a specified number of days. This script raises an event if the number of inactive public folders exceeds the threshold you set.

This script helps you manage infrequently accessed information resources that can, over time, consume valuable resources.

Note
This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information about setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Microsoft Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of inactive public folders exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of inactive public folders. The default is n.
Inactive after N days	Specify the number of days to use as a measure of whether a public folder is inactive. The default is 10 days.
Maximum threshold for number of inactive folders	Specify the maximum number of public folders that can be inactive before an event is raised. The default is 300 inactive public folders.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.

Description	How to Set It
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of inactive public folders exceeds the threshold.The default is 5 (red event indicator).

ISConnections

Use this Knowledge Script to monitor both the number of active connections and the total number of connections to the information store. This script raises an event if the number of either the active or the total connections is over the threshold for the specified consecutive number of intervals.

Resource Object

Information Store folder

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • Total connections • Active connections The default is n.
Maximum threshold for total number of connections	Specify the maximum total number of connections to the information store that can occur before an event is raised. The default is 100 connections.
Maximum threshold for number of active connections	Specify the maximum number of information store connections that can be active before an event is raised. The default is 100 connections.
Consecutive number of times before an event	Specify the consecutive number of intervals during which the threshold for connections can be exceeded before the script raises an event. The default value is 5 consecutive intervals. Because connections can have periodic spikes, you can set this parameter to a higher value to filter out unnecessary events. For example, you can allow the number of active connections to exceed the threshold 3 to 4 times before an event is raised.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ISLogFileSize

Use this Knowledge Script to monitor the size of transaction logs and the reserved transaction log files on Exchange 2000 Server or Exchange Server 2003. This script raises an event if the size of the transaction logs exceeds the threshold you set.

Resource Object

Microsoft Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the size of the transaction logs exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the log file size in MB. The default is n.
Maximum threshold for log file size (MB)	Specify the maximum size the transaction logs can attain before an event is raised. The default is 400 MB.
Logs you want to monitor	Specify one of the following values to specify the log you want: • **EDB** specifies transaction log. • **RES** specifies reserved transaction log. • **ALL** specifies both logs listed above. The default, ALL, monitors all logs for the Exchange version.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the size of the transaction logs exceeds the threshold. The default is 5 (red event indicator).

ISMailboxStoreAvgDlvryTime

Use this Knowledge Script to monitor the average time between the submission of a message to a mailbox store and the subsequent delivery of the message to local recipients (on the same server) or to other storage providers. This script reports the average delivery time for the last ten messages. This script raises an event if the average delivery time to local recipients or other storage providers exceeds the thresholds you set.

This script helps you manage the performance of mailbox stores.

Resource Object

Information Store folder, Mailbox Store object

Default Schedule

The default interval is **Every 3600 seconds**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the average delivery time to other storage providers, and the average local delivery time for the mailbox store. The default is n.
Maximum threshold for the rate at which messages are delivered locally	Specify the maximum rate at which messages can be delivered locally before an event is raised. The default is 500 deliveries per second.
Maximum threshold for the rate that requests to open folders are submitted to the information store.	Specify the maximum rate at which requests to open folders can be submitted before an event is raised. The default is 500 submissions per second.
Maximum threshold for the rate that requests to open messages are submitted to the information store.	Specify the maximum rate at which requests to open messages can be submitted before an event is raised. The default is 500 submissions per second.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ISMailboxStoreOpens

Use this Knowledge Script to monitor the number of requests per second submitted to the information store to open a mailbox store. If the rate of requests to open a mailbox store increases, it may indicate increased demand on the Exchange 2000 server or increased user activity. This script raises an event if the number of requests per second exceeds the threshold you set.

Resource Object

Information Store folder, Mailbox Store object

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of mailbox open requests received per second. The default is n.
Maximum threshold for number of folder requests	Specify the maximum rate at which folder requests can be submitted before an event is raised. The default is 100 requests per second.
Maximum threshold for number of message requests	Specify the maximum rate at which message requests can be submitted before an event is raised. The default is 100 requests per second.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ISMailboxStoreSize

Use this Knowledge Script to monitor the disk space used by a mailbox store. This script raises an event if the size of a monitored mailbox store, a Microsoft Access Database (MDB) file, exceeds the threshold you set.

Resource Object

Information Store folder, Mailbox Store object

Default Schedule

The default interval is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the size of a mailbox store exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the file size, in megabytes, of the specified mailbox store. The default is n.
Maximum threshold for size of mailbox store (MB)	Specify the maximum size a mailbox store can attain before an event is raised. The default is 4000 MB.
MDB files to monitor (EDB, Stream, or ALL)	Specify the mailbox store files you want to monitor: • **EDB** monitors regular message data. • **Stream** monitors streaming message data. • **ALL** monitors regular and streaming message data. The default is ALL.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which the size of mailbox store exceeds the threshold. The default is 5 (red event indicator).

ISPubStoreAvgDeliveryTime

Use this Knowledge Script to monitor the average time between the submission of a message to a public store and the subsequent delivery of the message to local recipients (on the same server) or other storage providers. This script reports the average delivery time for the last ten messages. This script raises an event if the average delivery time to local recipients or other storage providers exceeds the thresholds you set.

This script helps you manage the performance of public stores.

Resource Object

Information Store folder, Public Store object

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the average local delivery time and the average delivery time to other providers for the public store. The default is n.
Maximum threshold for average delivery time to local recipients	Specify the maximum average delivery time to local recipients that can occur before an event is raised. The default is 500 seconds.
Maximum threshold for average delivery time to storage providers	Specify the average delivery time to other storage providers that can occur before an event is raised. The default is 500 seconds.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ISPubStoreOpens

Use this Knowledge Script to monitor the number of requests per second submitted to the information store to open a public store. If the rate of requests to open a public store increases, it may indicate increased demand on the Exchange 2000 server or increased user activity. This script raises an event if the number of requests per second exceeds the threshold you set.

Resource Object

Information Store folder, Public Store object

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of folders opened per second. The default is n.
Maximum threshold for number of folder requests	Specify the maximum rate at which requests to open folders can be submitted before an event is raised. The default is 100 requests per second.
Maximum threshold for number of message requests	Specify the maximum rate at which requests to open messages can be submitted before an event is raised. The default is 100 requests per second.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ISPubStoreSize

Use this Knowledge Script to monitor the disk space used by any public store in the TreeView. This script raises an event if a monitored public store, a Microsoft Access Database (MDB) file, exceeds the threshold you set.

Resource Object

Information Store folder, Public Store object

Default Schedule

The default interval is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the size of a public store exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the size, in megabytes, of the public store. The default is n.
Maximum threshold for size public store (MB)	Specify the maximum size a public store can attain before an event is raised. The default is 4000 MB.
MDB files you want to monitor (EDB, Stream, or ALL)	Specify the public store files you want to monitor: • **EDB** monitors regular message data. • **Stream** monitors streaming message data. • **ALL** monitors regular and streaming message data. The default is ALL.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which the size of a public store exceeds the threshold. The default is 5 (red event indicator).

LinkStatus

Use this Knowledge Script to monitor the status of all link queues for all X.400 and SMTP virtual servers, including the number, size, and elapsed time for messages that reside in a link queue. This script monitors the link queue status at each monitoring interval and gives you a "snapshot" of the link queue status.

In Exchange 2000 or Exchange Server 2003, messages with the same next-destination server are transferred into the same queue. This queue is known as a *link queue*. Messages reside in the link queue until an active connection is made with the next-destination server, and that server agrees to process the messages.

Note
Although system queues are always visible, link queues may disappear after all messages have been sent to the next-destination server. The link queue will appear again when new messages are queued.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Once a day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Specify a protocol (X400, SMTP, or ALL)	Specify the protocol you want to monitor (not case-sensitive): • **X400** monitors the X.400 protocol. • **SMTP** monitors the SMTP protocol. • **ALL** monitors both X.400 and SMTP protocols. The default is ALL.
Collect total number of messages, link size and elapsed time of links?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of messages, link size, and elapsed time that messages reside in a link queue. The default is n. Use the parameters that follow to monitor or change the default event thresholds for the total number of messages, link size, or elapsed time that messages reside in a link queue.
Collect data for number of messages in links?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of messages in a link queue. The default is n.
Maximum threshold for number of messages in links	Specify the maximum number of messages that can be in a link queue before an event is raised. The default is 1000.
Event for number of messages in links?	Set to **y** to raise an event when the server exceeds the threshold for number of messages. The default is y.
Event severity: Number of messages in links	Set the event severity level, from 1 to 40, to specify the importance of an event in which the number of messages in the link queue exceeds the threshold. The default is 5 (red event indicator).

Description	How to Set It
Collect data for size of links?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the size of a link queue. The default is n.
Maximum threshold for size of links	Specify the maximum size a link queue can attain before an event is raised. The default is 100 MB.
Event for size of links?	Set to **y** to raise an event if the size of a link queue exceeds the threshold. The default is y.
Event severity: Size of links	Set the event severity level, from 1 to 40, to specify the importance of an event in which the size of a link queue exceeds the threshold. The default is 5 (red event indicator).
Collect data for elapsed time in links?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the oldest messages in a link queue. The default is n.
Maximum threshold for elapsed time in links	Specify the maximum amount of time that a message can remain in a link queue before an event is raised. The default is 1000 seconds.
Event for elapsed time in links?	Set to **y** to raise an event if a message exceeds the threshold for elapsed time in a link queue. The default is y.
Event severity: Elapsed time in links	Set the event severity level, from 1 to 40, to specify the importance of an event in which a message exceeds the threshold for elapsed time in a link queue. The default is 5 (red event indicator).

LogParser

Use this Knowledge Script to execute a query against Exchange log files and return those results in an event message or in a data stream. This script invokes Microsoft Log Parser, which uses Structured Query Language (SQL) to process Exchange log files. Microsoft Log Parser executes your query on the Exchange logs on the monitored Exchange server.

You build your query statement using Query Builder, which you access from the *Launch Query Builder* parameter on the Values tab. For more information, see "Using Query Builder" on page 67.

This script raises an event if the number of matches to your query exceeds the threshold you set.

You can save the results of the query to a comma-separated values (.csv) file in a location you specify on the monitored Exchange server.

Prerequisite

Microsoft Log Parser version 2.2 installed on the monitored Exchange server and on each console computer where you will use Query Builder. You can download Microsoft Log Parser from the Microsoft Download Center.

Resource Object

Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval for this Knowledge Script is **Run Once**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event Notification	
Create event if matches are found?	Set to **Yes** to raise an event if the number of matches to your query exceeds the value you set for the *Threshold for matching lines* parameter. The default is Yes.
Severity - Matches found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of matches to your query exceeds the threshold you set. The default is 15.
Maximum number of records to display	Specify the maximum number of records to display in the event's Messages tab. If *Collect data?* is set to Yes, then this value also controls the number of records displayed in the data detail. The default is 25.
Threshold for matching lines	Specify the maximum number of matching lines that a query can return before an event is raised. The default is 0.
Create event if no matches are found?	Set to **Yes** to raise an event if no matches to your query are returned. The default is unchecked.

Description	How to Set It
Severity - No matches found	Set the event severity level, from 1 to 40, to indicate the importance of an event in which no matches to your query are returned. The default is 20.
Severity - Job failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the LogParser job fails. The default is 5. **Note** Invalid SQL syntax in your query statement can cause the LogParser job to fail. The event detail message will identify the failure.
Data Collection	
Collect data?	Set to **Yes** to collect data for charts and reports. If enabled, data collection returns one data stream based on the parsed result set. The default is unchecked. Each data point in a data stream contains the number of matched rows for that iteration of the script. The data detail contains a list of the records that matched your query, based on the value you set in the *Maximum number of records to display* parameter.
Monitoring	
Query building process	Select the way you want to build your query in the Query Builder dialog box: • Select **Manual** to type your own SQL query statement in the Query Builder dialog box. • Select **Query tool** to use the interactive elements (such as lists and check boxes) of the Query Builder dialog box to build your SQL query statement. The default is Query tool.
Launch Query Builder	Click **Browse [...]** to open the Query Builder dialog box and build your query. For more information, see "Using Query Builder" on page 67.
Scan entire file at each iteration?	Set to **Yes** to scan the entire log file at every iteration of the Knowledge Script job. The default is unchecked. If this option is not selected, the first iteration of the Knowledge Script job places a marker at the end of the log file. During a subsequent iteration, the script scans the log file from the marked point and processes new log entries only.
Save query results to a file?	Set to **Yes** to save the entire results of your query to a .csv file. Use the *Full path to results file* parameter to indicate where you want to save the results file. The default is unchecked.
Full path to results file	Specify the full path to the location in which you want to save the results .csv file. The default location is `C:\Program Files\NetIQ\Temp\`.

Using Query Builder

Query Builder is a component of the LogParser Knowledge Script that allows you to build complex SQL queries manually or with the help of the Query tool. Use Query Builder to construct your query before running LogParser.

Building a Query with the Query Tool

You can simplify the process of building a SQL query by choosing **Query tool** in the *Query building process* parameter in the LogParser Knowledge Script, and then clicking **Browse [...]** in the *Launch Query Builder* parameter.

Notes

- Microsoft Log Parser version 2.2 must be installed on the monitored Exchange server and on each console computer where you will use Query Builder.
- For examples of building a query with the Query tool, see "Using the Query Tool - Example 1" on page 70 and "Using the Query Tool - Example 2" on page 70.

To build a query using the Query tool in Query Builder:

1. Build your SQL query in Query Builder according to the field descriptions in the table below.
2. When you have finished building your query, click **OK**. Query Builder returns your query statement to the LogParser Knowledge Script.

Field	Description
Type of Log	Query Builder uses the W3C Log File format. You cannot change the selection.
Sample Log File	Click **Browse** to select a log file that is an *example* of the log file you want to query. You can use the built-in sample file, which ships with AppManager for Exchange 2000 or 2003 and is installed by default on your local system at `C:\Program Files\NetIQ\AppManager\bin\SampleExchLogFile.log`. Query Builder uses the column names in the sample log file to populate the contents of the Column List field.
Log File Path on Server	Specify the full path to the location of the Exchange log you want to query. This field is disabled when the **Auto Detect Log File Path** option is enabled. To manually specify a log location, you must first enable **Auto Detect Log File Path**. The path is displayed in the Query Statement section as the "From" statement in your query. For example: `From C:\program Files\exchsrvr\LabServer.log` **Tip** If you want to run the LogParser script on several Exchange servers, and the path to the Exchange log is the same for each server, you can use the `{Server Name}` variable in the file path. By default, the names of Exchange logs contain the name of the server. Therefore, when searching for your Exchange log, AppManager replaces the variable with the name of the server on which you run the LogParser script. For example, type `C:\Program Files\exchsrvr\{Server Name}.log`
Auto Detect Log File Path	This option is the preferred method for identifying the Exchange log to query. Select to automatically detect the location of the Exchange log on the monitored Exchange server. The LogParser Knowledge Script determines the Exchange log directory based on the configuration of the Exchange server. Your selection is displayed in the Query Statement field as the "From" statement in your query. For example: `From {Auto Detect}\*.log`
Column List	Contains a list of the columns in the sample log file. Select the columns that you want to use in your query. Your selections are displayed in the **Columns** field in the Criteria section and in the Query Statement field as the "Select" statement of your query. For example: `Select client-ip,Client-hostname,message-subject` For more information about what each column contains, see "Understanding Log File Columns" on page 73.

Field	Description
Criteria	Use the fields in this section to customize your query. Your selections are displayed in the Query Statement section.
Show	Select to include the associated column in your query statement. Clear to remove the associated column from your query statement. Although the column is removed from the statement, it is not removed from the Criteria section.
Columns	This field is automatically populated by your selections in the **Column List** field. Your selections are displayed in the Query Statement section as the “Select” statement in your query. For example: `Select total-bytes` **Tip** You can click in a blank field in this column to select a column name to include in the query. This feature is helpful if you want to set multiple conditions on the same column: select the same column name in two or more fields and then customize each row for each separate set of query operators and keywords.
Group By	Allows you to perform aggregate functions, such as SUM, for selected column values, rather than for the entire column. Select the function you want to perform: • Sum • Count • Max • Min • Avg Your selection is displayed in the Query Statement section as part of the “Select” statement in your query. For example: `Select Avg(total-bytes)`
Rename To	Provide a new name for the column to display in the results. This feature allows you to display an alternative column name in the query results. The new name is displayed in the Query Statement section as part of the “Select” statement in your query. For example: `Select Avg(total-bytes) As Average Total Bytes`
Sort Type	Select **Ascending** or **Descending** to sort the results for the associated column name. Your selection is displayed in the Query Statement section as part of the “Order By” statement in your query. For example: `Order By Date Asc`
Grouping	Select to group query results by the associated column name. Your selection is displayed in the Query Statement section as part of the “Group By” statement in your query. For example: `Group By Date`
Operator	Select a method for filtering log entries based on one or more conditions. • **>** finds log entries that are greater than the specified condition. • **<** finds log entries that are less than the specified condition. • **=** finds log entries that match the specified condition. • **>=** finds log entries that are greater than or match the specified condition. • **<=** finds log entries that are less than or match the specified condition. • **NOT** finds log entries that *do not* match the specified condition. • **LIKE** allows you to use wildcards to find log entries for the specified condition. -- Use the % wildcard to match a text string of any length -- Use the _ wildcard to match a single character Your selection is displayed in the Query Statement section as part of the “Where” statement in your query. For example: `Where Date = 20080925`

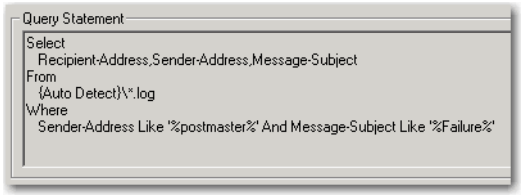
Field	Description
Condition	Type the value you want to compare for the associated column. Your selection is displayed in the Query Statement section as part of the "Where" statement in your query. For example: `Where Date = 20080925` If you selected **LIKE** in the **Operator** field, use the wildcard along with your value in the **Condition** field. **Note** If the associated column supports the "String" type, rather than an "Integer," a "Timestamp," or a "Real" type, enclose your condition text in single quotes, for example: `'production-server'`.
Remove	Click to remove the associated column from your query statement *and* from the Criteria section. This action also clears the column name in the **Column List** field.
Query Statement	As you select information in the fields in Query Builder, the Query Statement section reflects the selections you make in SQL query syntax. You cannot change information directly in the Query Statement section. Yyou must do so by changing your selections in the Criteria section. **Tip** If a query statement you build with Query Builder is not as complex as you need it to be, you can copy the contents of the Query Statement section and use the manual query option. From there, you can manually complete your query. For more information, see "Building a Query Manually" on page 72.

Using the Query Tool - Example 1

In the following example, use the Query Tool to build a query that will look for Exchange log entries for which the recipient has received email messages that contain the word "Failure" in the message subject and were sent from the postmaster. Depending on your threshold and data collection selections, the LogParser Knowledge Script event message and data details return the column entries that match the conditions you set.

To build query example 1:

1. Accept the default values for the **Type of Log** and **Sample Log File** fields.
2. Select **Auto Detect Log File Path**.
3. In the **Column List** field, select **Recipient-Address**, **Sender-Address**, and **Message-Subject**.
4. In the **Operator** field for the Sender-Address column, select **LIKE**.
5. In the **Condition** field for the Sender-Address column, type `'%postmaster%'`.
6. In the **Operator** field for the Message-Subject column, select **LIKE**.
7. In the **Condition** field for the Message-Subject column, type `'%Failure%'`. The Query Statement field contains the following query statement:



8. Click **OK**.

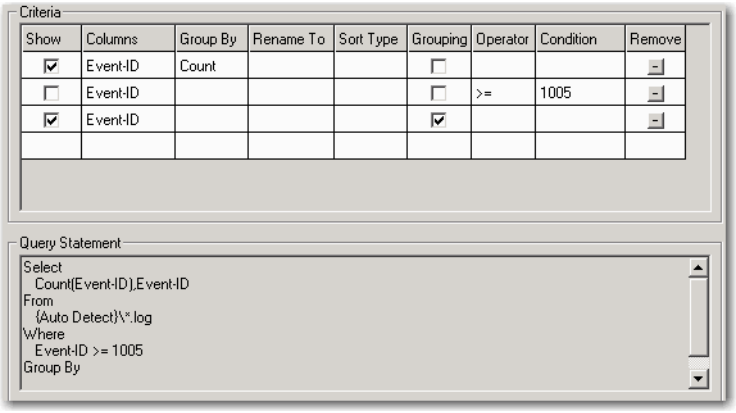
Using the Query Tool - Example 2

In the following example, you use the Query Tool to build a query that uses multiple instances of the same column.

The purpose of this query is to return a count of all Event ID values greater than or equal to 1005 and group them by Event ID value.

To build query example 2:

1. Accept the default values for the **Type of Log** and **Sample Log File** fields.
2. Select **Auto Detect Log File Path**.
3. In the **Column List** field, select **Event-ID**. A row for the Event-ID column is displayed in the **Criteria** field.
4. In the blank row below the Event-ID row, click in the **Columns** field and select **Event-ID** to create a second row for the Event-ID column.
5. Repeat step 4 to create a third row for the Event-ID column.
6. Note that for all rows, **Show** is selected. Clear **Show** for the second, or middle, row to remove it from the Select statement.
7. In the first row, select **Count** in the **Group By** field.
8. In the second row, the row for which **Show** is cleared, select **>=** (greater than or equal to) in the **Operator** field and type `1005` in the **Condition** field.
9. In the third row, select **Grouping**. Your completed query should look like this:



10. Click **OK**.

The LogParser Knowledge Script event message and data details return the count of Event-ID values greater than or equal to 1005 grouped by the Event-ID value, as illustrated in the following picture.

Log Parser Query Result

COUNT(ALL Event-ID)	Event-ID
831	1019
1097	1025
1097	1024
1097	1033
962	1034
133	1030
135	1036
135	1023
135	1028
132	1021
2	1027
652	1020
652	1031

Building a Query Manually

You can manually build a SQL query by choosing **Manual** in the *Query building process* parameter in the LogParser Knowledge Script, and then clicking **Browse [...]** in the *Launch Query Builder* parameter.

To build a query manually in Query Builder:

1. Build your query in Query Builder according to the field descriptions. If you do not have Microsoft Log Parser 2.2 installed, only the **Query Statement** field is displayed in the dialog box.

Field	Descriptions
Type of Log	Query Builder uses the W3C Log File format. You cannot change this selection.
Sample Log File	Click **Browse** to select a log file that is an *example* of the log file you actually want to query. You can use the built-in sample file, which ships with AppManager for Exchange 2000 or 2003 and is installed by default on your local system at `C:\Program Files\NetIQ\AppManager\bin\SampleExchLogFile.log`.
Column List	Contains a list of the columns in the sample log file. Refer to these column names when building your query statement. For more information about what each column contains, see "Understanding Log File Columns" on page 73.
Query Statement	Using standard SQL query syntax, type your query statement. For more information, see "Building a Query Manually" on page 72.

2. When you have finished building your query, click **OK**. Query Builder returns the query statement to the LogParser Knowledge Script.

Manually Building a Query - Example

The Query Builder Query tool does not support expressions such as "In." To use the "In" condition, you must manually build a query. The following example details the process of building a query that parses the Exchange log for specified Event IDs. The LogParser Knowledge Script event message and data details return the column entries that match the conditions you set.

To build the manual query example:

1. In the **Query Statement** field, type the following Select statement to identify the columns you want to include in your query.

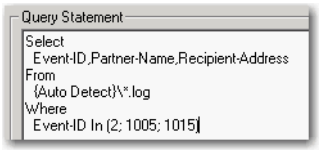
   ```
   Select Event-ID,Partner-Name,Recipient-Address
   ```

2. To enable AppManager to automatically find the Exchange log you want to parse, type `From {Auto Detect}\*.log`.

3. Type the following Where statement to identify the Event IDs you want to find in the Exchange log.

   ```
   Where Event-ID In (2; 1005; 1015)
   ```

   The completed query statement looks similar to the following:

4. Click **OK**.

Understanding Log File Columns

Use the information provided in this section to build queries for the LogParser Knowledge Script, which supports Exchange log file formats. The following table provides the Microsoft descriptions for the column names in Exchange log files:

Column Name	Type	Description
Date	STRING	The date of the event.
Time	STRING	The Greenwich mean time of the event.
client-ip	STRING	The IP of connecting client.
Client-hostname	STRING	The hostname of connecting client.
Partner-Name	STRING	The name of the messaging service that the message is handed off to. In Exchange 2000, the service can be: SMTP, X400, MAPI, IMAP4, POP3, STORE. This is essentially the same as Exchange Server 5.5, but in Exchange 2000, there are more possibilities for this field.
Server-hostname	STRING	The hostname of the server that makes the log entry.
server-IP	STRING	The IP address of the server that makes the log entry.
Recipient-Address	STRING	The message recipient (SMTP or X.400 address).
EventID	INTEGER	An integer value corresponding to the Event Type of the logged actions such as sent, received, delete, retrieve.
MSGID	INTEGER	The message ID.
Priority	INTEGER	The priority level, represented by -1 if low, 0 if normal, 1 if high.
Recipient-Report-Status	INTEGER	A number representing the result of an attempt to deliver a report to the recipient: 0 if delivered, 1 if not delivered. This is used only for non-delivery reports (NDRs) and delivery reports (DRs). On other events, it is blank.
total-bytes	INTEGER	The message size in bytes.
Number-Recipients	INTEGER	The total number of recipients.
Origination-Time	STRING	The delivery time (in seconds) representing the time it takes to deliver the message. This is determined from the difference between the timestamp and time encoded in Message ID. This is only valid for messages within the Exchange organization (all versions). There is no requirement to decode other product message IDs such as Sendmail.
Encryption	INTEGER	The encryption level (For the primary body part: 0 if there is no encryption, 1 if signed, 2 if encrypted. This is per message, not per recipient).
service-Version	STRING	The version of the service making the log entry.
Linked-MSGID	STRING	If there is a MSGID from another service, it is given here to link the message across services.
Message-Subject	STRING	The subject of the message, truncated to 256 bytes.
Sender-Address	STRING	The primary address of the originating mailbox, if known. This could be SMTP, X.400, or Distinguished Name (DN), depending on the transport.

MailboxesOverStorageLimit

Use this Knowledge Script to monitor the number of mailboxes over the storage limit. This script provides useful report data to help you manage Exchange mailboxes.

On a computer with more than one virtual server, the total number of mailboxes over the storage limit is calculated as the total number of mailboxes over the storage limit for all virtual servers on the computer.

If a failover occurs when this script job is running, the job restarts on the new node. It is normal for the job on the failed node to generate one or more error messages, depending on what it was doing when the failover occurred.

Note
This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of mailboxes over the storage limit exceed the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of mailboxes that exceed the storage limit. The default is n.
Maximum threshold for number of mailboxes	Specify the maximum number of mailboxes that can exceed their storage limit before an event is raised. The default is 300 mailboxes.
Exchange profile for NetIQ Corporationmc log on as account	Enter a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.

Description	How to Set It
Mailbox alias for NetIQ Corporationmc log on as account	Enter a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default value is 5 (red event indicator).

MailboxesWithoutStorageLimit

Use this Knowledge Script to monitor the number of mailboxes with no storage limitation. This script provides useful report data to help you manage Exchange mailboxes.

On a computer with more than one virtual server, the total number of mailboxes without a storage limit is calculated as the total number of mailboxes without a storage limit for all virtual servers on the computer.

If a failover occurs when this script job is running, the job restarts on the new node. It is normal for the job on the failed node to generate one or more error messages, depending on what it was doing when the failover occurred.

Note

This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of mailboxes with no storage limitation exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of mailboxes with no storage limit. The default is n.
Maximum threshold for number of mailboxes	Specify the maximum number of mailboxes that can have no storage limit before an event is raised. The default is 300 mailboxes.
Exchange profile for NetIQ Corporationmc log on as account	Enter a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Mailbox alias for NetIQ Corporationmc log on as account	Enter a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of mailboxes with no storage limit exceeds the threshold. The default value is 5 (red event indicator).

MailboxStoreMountStatus

Use this Knowledge Script to monitor the mount status of one or more mailbox stores. When a mailbox store is unmounted, the Exchange Server cannot store information in it or read information from it.

Resource Object

Information Store folder, Mailbox Store object

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a mailbox store is unmounted. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns 100 if the mailbox store is mounted, 0 if the mailbox store is unmounted. The default option is n.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a mailbox store is unmounted. The default is 5 (red event indicator).

MsgAvgLocalDlvryTimeByIntrv

Use this Knowledge Script to monitor the average delivery time for local messages since the last time the script ran.

Tracking logs are implemented using the network share `<servername>.log`. This shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if average delivery time exceeds the threshold. The default is y.
Collect averages data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the average delivery time since the last time the script ran. The default is n.
Collect totals data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of messages and the total elapsed deliver time from which the average was derived. The default is n.
Maximum threshold for the average local delivery time.	Specify the highest average amount of time that it can take for local messages to be delivered before an event is raised. The default is 300 seconds.
Date format in message tracking log	Set this to be the same as the date format you are using in your message tracking log. The default is YYYY-MM-DD.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which average delivery time exceeds the threshold you set. The default is 5 (red event indicator).

MsgsAvgLocalDeliveryTime

Use this Knowledge Script to monitor the average delivery time for local messages for specified days. You can specify the interval to be a number of past days or start and stop dates.

Either interval specification looks at entries in the message tracking logs for the indicated days. If *Past N days to average messages* is 1, it looks at all the entries in today's log, since midnight, when it started, regardless of what time of day it is now. If *Past N days to average messages* is 2, it also examines the log from the day before that (all 24 hours of it).

Tracking logs are implemented using the network share `<servername>.log`. This shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share.

This script reports 0 messages transferred if you delete or disable the tracking logs.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if average delivery time exceeds the threshold you set. The default is y.
Collect averages data?	Set to **y** to collect data for charts and reports. If enabled data collection returns the average delivery time over the monitoring interval. The default is n.
Collect totals data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of messages and the total elapsed deliver time from which the average was derived. The default is n.
Maximum threshold for the average local delivery time.	Specify the maximum average delivery time that can have occurred since the last time this script was run. The default is 120 seconds.
Past N days to average messages	Specify the number of days over which to calculate the average delivery time. This value is ignored if you specify start and end dates. The default is 3 days.
Start date (YYYY/MM/DD)	Specify the start date for averaging delivery times.
End date (YYYY/MM/DD)	Specify the end date for averaging delivery times.
Date format in message tracking log	Set this to be the same as the date format you are using in your message tracking log. The default format is YYYY-MM-DD.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which local delivery time exceeds the threshold. The default is 5 (red event indicator).

MsgsBetweenAdminGroups

Use this Knowledge Script to monitor the total number and size of messages transferred between Exchange Admin Groups during the specified number of days or between specific start and end dates.

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log`. This shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Note
Daily Exchange server logs begin and end at midnight using Coordinated Universal Time (UTC) rather than local time. The UTC standard is equivalent to Greenwich Mean Time (GMT). This Knowledge Script also uses GMT and does not adjust for your time zone. Depending on your time zone, the number of days in local time may not represent the corresponding number of GMT hours. For example, if you monitor the previous day's messages (Count messages from past N days is set to 1), and your time zone is GMT -08:00 (Pacific Time), running the Knowledge Script job at 09:00 will monitor only 16 hours of the day's Exchange server log recorded in GMT. If your time zone is GMT, your results will be accurate.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event when a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • Number of e-mail messages received from other Admin Groups. If this Knowledge Script cannot identify the Admin Group to which the sender belongs, the data detail message indicates the "Admin Group of <sender>". • Size of messages received in KB. • Number of e-mail messages sent to other Admin Groups. If this Knowledge Script cannot identify the Admin Group to which the recipient belongs, the data detail message indicates the "Admin Group of <recipient>". • Size of messages sent in KB. The default is n.
Maximum threshold for number of received mail messages	Specify the maximum number of messages that can be received from remote Admin Groups before an event is raised. The default is 300 messages.

Description	How to Set It
Maximum threshold for number of sent mail messages	Specify the maximum number of messages that can be sent from this Admin Group to other Admin Groups before an event is raised. The default value is 300 messages.
Include Exchange system messages?	Set to **y** to include system messages in the message count. The default is n.
Count messages from past N days	Specify the number of previous days (including today) to track back for the message count. For example, to find the number of messages transferred in the past week, enter 7. The default value is 3 days. To set a specific start date and end date, leave this field blank. If you set a start and end date, this parameter is ignored.
Start date (YYYY/MM/DD)	Specify a start date for beginning the message count. If you do not specify a Start and End Date, the value for *Count messages from past N days* is used.
End date (YYYY/MM/DD)	Specify the end date for the message count. If you do not specify a Start and End Date, the value for *Count messages from past N days* is used.
Refresh server info at each interval?	Set to **y** to generate a table showing the Microsoft Exchange 2000 or Exchange Server 2003 servers and the admin groups to which they belong. In large organizations with hundred of servers, creating this table may take a while. Therefore, this parameter allows you to decide whether to create the table every time the script runs. If the customer environment is pretty static, there is little need to create the table. On the other hand, if the customer environment is very dynamic and the servers are moved across different admin groups quite often, then it is preferable to set this parameter to **y**. The default is n.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

MsgsBtwnAdmnGrpsByInterval

Use this Knowledge Script to monitor the number and size of messages sent to an Exchange Admin Group or received from an Exchange Admin Group during the monitoring interval.

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log`. This shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns data collected during the monitoring interval: • Number of mail messages received from other Admin Groups. If this Knowledge Script cannot identify the Admin Group to which the sender belongs, the data detail message indicates the "Admin Group of <sender>". • Size of messages received in KB • Number of mail messages sent to other Admin Groups. If this Knowledge Script cannot identify the Admin Group to which the recipient belongs, the data detail message indicates the "Admin Group of <recipient>". • Size of messages sent in KB The default is n.
Maximum threshold for number of received mail messages	Specify the maximum number of messages that can be received from remote Admin Groups before an event is raised. The default is 300 messages.
Maximum threshold for number of sent mail messages	Specify the maximum number of messages that can be sent from this Admin Group to other Admin Groups before an event is raised. The default is 300 messages.
Include Exchange system messages?	Set to **y** to include system messages in the message count. The default is n.

Description	How to Set It
Refresh server info at each interval?	Set to **y** to generate a table showing the Microsoft Exchange 2000 or Exchange Server 2003 servers and the admin groups to which they belong. In large organizations with hundred of servers, creating this table may take a while. Therefore, this parameter allows you to decide whether to create the table every time the script runs. If the customer environment is pretty static, there is little need to create the table. On the other hand, if the customer environment is very dynamic and the servers are moved across different admin groups quite often, then it is preferable to set this parameter to **y**. The default is n.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

MsgsByServer

Use this Knowledge Script to monitor the number and size of messages transferred between a target Exchange Server and all connected servers during a specified number of days or from a specific start date to a specific end date.

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log` in Exchange 2000 or Exchange Server 2003 and `tracking.log` in earlier versions. The shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share. If you install Exchange server on a Microsoft cluster, make sure the network share exists on all cluster nodes.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Note
Daily Exchange server logs begin and end at midnight using Coordinated Universal Time (UTC) rather than local time. The UTC standard is equivalent to Greenwich Mean Time (GMT). This script also uses GMT and does not adjust for your time zone. Depending on your time zone, the number of days (in local time) may not represent the corresponding number of GMT hours. For example, if you monitor the previous day's messages (Count messages from past N days is set to 1), and your time zone is GMT -08:00 (Pacific Time), running the Knowledge Script job at 09:00 will monitor only 16 hours of the day's Exchange server log recorded in GMT. If your time zone is GMT, your results will be accurate.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • Size (KB) of messages sent • Number of messages sent • Size (KB) of messages received • Number of messages received The default is n.
Maximum threshold for number of received mail messages	Specify the maximum number of messages that can be received from remote server before an event is raised. The default is 300 messages.
Maximum threshold for number of sent mail messages	Specify the maximum number of messages that can be sent from this server to other servers before an event is raised. The default is 300 messages.
Include Exchange system messages?	Set to **y** to include system messages in the message count. The default is n.

Description	How to Set It
Count messages from past N days	Enter the number of previous days (including today) to track back for the message count. For example, to find the number of messages transferred in the past week, enter 7. The default is 3 days. To set a specific start date and end date, leave this field blank. If you set a start and end date, this parameter is ignored.
Start date	Specify a start date for beginning the message count. Use the YYYY/MM/DD format.
End date	Specify a end date for the message count. Use the YYYY/MM/DD format.
Refresh server info at each interval (Exchange 2000 or Exchange 2003 only)?	Specify whether this script should dynamically create a table that describes which Exchange servers belong to which admin groups at each interval. In large organizations, creating this table can take a significant period of time. Therefore, decide whether to create the table every time the script runs based on the characteristics of your Exchange environment: • If your environment tends to remain static with few (if any) changes, you should not need to create the table and can set this parameter to **n**. • If your environment tends to be dynamic, with servers often moved from one admin group to another, you should set this parameter to **y**. The default is n.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

MsgsByServerByInterval

Use this Knowledge Script to monitor the number and size of messages transferred between a target Exchange Server and all connected servers during the monitoring interval.

In the parameters described below, the term "messages received" refers to the messages that the target Exchange Server received. "Messages sent" refers to the messages that the target Exchange Server sent to all connected Exchange Servers.

To use this script, you must enable the Tracking logs. Tracking logs are implemented using the network share `<servername>.log` in Exchange 2000 or Exchange Server 2003 and `tracking.log` in earlier versions. The shared directory must exist on the target computer for this script to work properly. By default, the Exchange Server installation program sets up the share. If you install Exchange Server on a Microsoft cluster, make sure the network share exists on all cluster nodes.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns data collected during the monitoring interval: • Size (KB) of messages sent • Number of messages sent • Size (KB) of messages received • Number of messages received The default is n.
Maximum threshold for number of received mail messages	Specify the maximum number of messages the target Exchange server can receive before an event is raised. The default is 300 messages.
Maximum threshold for number of sent mail messages	Specify the maximum number of messages that can be sent from the target Exchange Server to connected Exchange Servers before an event is raised. The default is 300 messages.
Include Exchange system messages?	Set to **y** to include system messages in the message count. The default is n.

Description	How to Set It
Refresh server info at each interval (Exchange 2000 only)?	Specify whether this script should dynamically create a table that describes which Exchange 2000 or Exchange Server 2003 servers belong to which admin groups at each interval. In large organizations, creating this table can take a significant period of time. Therefore, decide whether to create the table every time the script runs based on the characteristics of your Exchange 2000 or Exchange Server 2003 environment: • If your environment tends to remain static with few (if any) changes, you should not need to create the table and can set this parameter to **n**. • If your environment tends to be dynamic, with servers often moved from one admin group to another, you should set this parameter to **y**. The default is n.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

MsgsBySize

Use this Knowledge Script to monitor the number of messages transferred in different size ranges over a specified number of days or from a specific start date to a specific end date. This script checks the size of messages sent and received during a specified period and tracks the number of messages by size.

This script provides useful report data to help you monitor message traffic on a daily or weekly basis.

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log` in Microsoft Exchange 2000 or Exchange Server 2003 and `tracking.log` in earlier versions. The shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share. If you install Exchange server on a Microsoft cluster, make sure the network share exists on all cluster nodes.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Note
Daily Exchange server logs begin and end at midnight using Coordinated Universal Time (UTC) rather than local time. The UTC standard is equivalent to Greenwich Mean Time (GMT). This Knowledge Script also uses GMT and does not adjust for your time zone. Depending on your time zone, the number of days (in local time) may not represent the corresponding number of GMT hours. For example, if you monitor the previous day's messages (Count messages from past N days is set to 1), and your time zone is GMT -08:00 (Pacific Time), running the Knowledge Script job at 09:00 will monitor only 16 hours of the day's Exchange server log recorded in GMT. If your time zone is GMT, your results will be accurate.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Range for message size (comma separated)	Specify the size ranges for tracking messages, specified in KB, separated by commas. For example, if you set the range to `10,50,100`, information is returned for the number of messages from 0-10 KB, 10-50 KB, 50-100 KB, and 100+ KB. The default range is 1,2,10,50,100,500.
Collect data for local messages (delivered)?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of locally delivered mail messages in each size category. The default is y.
Collect data for remote messages (received)?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of mail messages received from a non-local mailbox in each size category. The default is y.
Collect data for remote messages (sent)?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of mail messages sent to a non-local mailbox in each size category. The default is y.

Description	How to Set It
Count messages from past N days	Specify the number of previous days (including today) to track back for the message count. For example, to find the number of messages transferred in the past week, enter 7. The default value is 8 days. To set a specific start date and end date, leave this field blank. If you set a Start Date and End Date, this parameter is ignored.
Start date	Enter a start date for beginning the message count. Use the YYYY/MM/DD format.
End date	Enter an end date for the message count. Use the YYYY/MM/DD format.

MsgsOfSystem

Use this Knowledge Script to monitor the load of public folder replication messages between Microsoft Exchange sites and Microsoft Exchange 2000 or Exchange Server 2003 Admin Groups.

To replicate public folder information between sites or Admin Groups, Microsoft Exchange sends system messages. This script monitors the number and size of the Exchange system messages:

- Sent from the public information store to public information store on another Exchange site or Admin Group.
- Received by the public information store from the public information store on another Exchange site or Admin Group.

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log` in Exchange 2000 or Exchange Server 2003 and `tracking.log` in earlier versions. The shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share. If you install Exchange server on a Microsoft cluster, make sure the network share exists on all cluster nodes.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Note
Daily Exchange server logs begin and end at midnight using Coordinated Universal Time (UTC) rather than local time. The UTC standard is equivalent to Greenwich Mean Time (GMT). This Knowledge Script also uses GMT and does not adjust for your time zone. Depending on your time zone, the number of days (in local time) may not represent the corresponding number of GMT hours.

For example, if you monitor the previous day's messages (*Count messages from past N days* is set to **1**), and your time zone is GMT -08:00 (Pacific Time), running the Knowledge Script job at 09:00 will monitor only 16 hours of the day's Exchange server log recorded in GMT. If your time zone is GMT, your results will be accurate.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number or size of any kind of system messages exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number and size of inbound and outbound messages for public folder and directory replication. The default is n.
Maximum threshold for number of system messages	Specify the maximum number of system messages that can be sent or received by the public information store before an event is raised. The default is 3000 messages.

Description	How to Set It
Maximum threshold for size of system messages	Specify the maximum size (in KB) for system messages sent or received by the public information store. An event is raised if messages exceed this size The default is 3000 KB.
Count messages from past N days	Specify the number of previous days (including today) to track back for the message count. For example, to find the number of messages transferred in the past week, enter 7. The default value is 3 days. To set a specific start date and end date, leave this field blank. If you set a Start Date and End Date, this parameter is ignored.
Start date	Specify a start date for beginning the message count. Use the MM/DD/YY format.
End date	Specify an end date for the message count. Use the MM/DD/YY format.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

MsgsOpenedByOWA

Use this Knowledge Script to monitor the number of messages opened by Outlook Web Access (OWA). This script raises an event if the number of opened messages exceeds the threshold you set.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of messages opened by OWA exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the difference between the number of messages opened by OWA during the current monitoring interval and the number of messages opened during the previous monitoring interval. The default is n.
Compare to previous monitoring interval?	Set to **y** to compare the number of messages opened by OWA during the current monitoring interval with the number of messages opened by OWA during the previous monitoring interval. The default is y. **Note** If set to n, data collection returns *only* the number of messages opened by OWA during the current monitoring interval.
Maximum threshold for the number of messages	Specify the maximum number of messages that OWA can open before an event is raised. The default is 99 messages.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which the number of opened messages exceeds the threshold. The default is 5 (red event indicator).

MsgsSentByOWA

Use this Knowledge Script to monitor the number of messages sent by Outlook Web Access (OWA). This script raises an event if the number of messages sent exceeds the threshold you set.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of messages sent by OWA exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the difference between the number of messages sent by OWA during the current monitoring interval and the number of messages sent during the previous monitoring interval. The default is n.
Compare to previous monitoring interval?	Set to **y** to compare the number of messages sent by OWA during the current monitoring interval with the number of messages sent by OWA during the previous monitoring interval. The default is y. **Note** If set to n, data collection returns *only* the number of messages sent by OWA during the current monitoring interval.
Maximum threshold for the number of messages	Specify the maximum number of messages that OWA can send before an event is raised. The default is 99 messages.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which the number of sent messages exceeds the threshold. The default is 5 (red event indicator).

MsgsSpecificDomain

Use this Knowledge Script to monitor the total number and size of messages transferred through an Internet Mail Connector (IMC) to and from a specific domain during a specified number of days or from a specific start date to a specific end date. In Exchange 2000 and Exchange Server 2003, the IMC has been replaced by the SMTP service.

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log` in Exchange 2000 or Exchange Server 2003 and `tracking.log` in earlier versions. The shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share. If you install Exchange server on a Microsoft cluster, make sure the network share exists on all cluster nodes.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Note
Daily Exchange server logs begin and end at midnight using Coordinated Universal Time (UTC) rather than local time. The UTC standard is equivalent to Greenwich Mean Time (GMT). This Knowledge Script also uses GMT and does not adjust for your time zone. Depending on your time zone, the number of days (in local time) may not represent the corresponding number of GMT hours. For example, if you monitor the previous day's messages (Count messages from past N days is set to 1), and your time zone is GMT -08:00 (Pacific Time), running the Knowledge Script job at 09:00 will monitor only 16 hours of the day's Exchange server log recorded in GMT. If your time zone is GMT, your results will be accurate.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • Number of messages received from the specified domain(s) • Size of messages received from the specified domain(s) in KB • Number of messages sent to the specified domain(s) • Size of messages sent to the specified domain(s) in KB The default is n.
Maximum threshold for number of received messages	Specify the maximum number of messages that can be received from the specified domain before an event is raised. The default is 300 messages.
Maximum threshold for number of sent messages	Specify the maximum number of messages that can be sent from this site to the specified domain before an event is raised. The default is 300 messages.

Description	How to Set It
List of domain names (comma separated)	Provide the name of the domain you want to monitor. You can enter multiple domain names separated by commas. For example: `microsoft.com,netiq.com`
Count messages from past N days	Specify the number of previous days (including today) to track back for the message count. For example, to find the number of messages transferred in the past week, enter 7. The default value is 3 days. If you set a start and end date, this parameter is ignored.
Start date	Specify a start date for beginning the message count. Use the YYYY/MM/DD format.
End date	Specify an end date for the message count. Use the YYYY/MM/DD format.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

Example of How This Script is Used

You can use this Knowledge Script to check the number and size of mail messages from a specific Internet domain. For example, to check the number of messages to and from NetIQ Corporation Corporation in the last 30 days, you would enter netiq.com for the Domain name parameter and 30 for the *Count messages from past N days* parameter.

MsgsSpecificDomainByInterval

Use this Knowledge Script to monitor the total number and size of messages transferred through an Internet Mail Connector (IMC) to and from a specific domain during the monitoring interval. In Microsoft Exchange 2000 and Exchange Server 2003, the IMC has been replaced by the SMTP service.

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log` in Exchange 2000 or Exchange Server 2003 and `tracking.log` in earlier versions. The shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share. If you install Exchange server on a Microsoft cluster, make sure the network share exists on all cluster nodes.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the following data collected during the monitoring interval: • Size (KB) of messages sent to other domains • Number of messages sent to other domains • Size (KB) of messages received from other domains • Number of messages received from other domains The default is n.
Maximum threshold for number of received messages	Specify the maximum number of messages that can be received from remote domains before an event is raised. The default is 300 messages.
Maximum threshold for number of sent messages	Specify the maximum number of messages that can be sent to other domains before an event is raised. The default is 300 messages.
List of domain names (comma separated)	Provide the name of the domain you want to monitor. You can enter multiple domain names separated by commas. For example: `microsoft.com,netiq.com`
Include Exchange system messages?	Set to **y** to include system messages in the message count. The default is n.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default value is 5 (red event indicator).

MsgsThroughConnector

This Knowledge Script monitors the total number and size of messages sent and received by one or more specified connectors on an Exchange site or router group during a specified number of days or from a specific start date to a specific end date. For Microsoft Exchange 2000 or Exchange Server 2003, this script monitors connectors to external mail systems only.

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log` in Exchange 2000 or Exchange Server 2003 and `tracking.log` in earlier versions. The shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share. If you install Exchange server on a Microsoft cluster, ensure the network share exists on all cluster nodes.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Note
Daily Exchange server logs begin and end at midnight using Coordinated Universal Time (UTC) rather than local time. The UTC standard is equivalent to Greenwich Mean Time (GMT). This script also uses GMT and does not adjust for your time zone. Depending on your time zone, the number of days (in local time) may not represent the corresponding number of GMT hours. For example, if you monitor the previous day's messages (Count messages from past N days is set to 1), and your time zone is GMT -08:00 (Pacific Time), running the Knowledge Script job at 09:00 will monitor only 16 hours of the day's Exchange server log recorded in GMT. If your time zone is GMT, your results will be accurate.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number or size of messages sent from or received by monitored connectors exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • Size (KB) of messages received by connectors • Number of messages received by connectors • Size (KB) of messages sent by connectors • Number of messages sent by connectors The default is n.
Maximum threshold for number of received messages	Specify the maximum number of messages that can be received by monitored connectors before an event is raised. The default is 300 messages.
Maximum threshold for number of sent messages	Specify the maximum number of messages that can be sent to monitored connectors before an event is raised. The default is 300 messages.
Include Exchange system messages?	Set to **y** to include system messages in the message count. The default is n.
Count messages from past N days	Specify the number of previous days (including today) to track back for the message count. For example, to find the number of messages transferred in the past week, enter 7. The default value is 3 days. To set a specific start date and end date, leave this field blank. If you set a Start Date and End Date, this parameter is ignored.
List of connectors (comma separated)	Provide a list of connector names, separated by commas. The connector name is not case-sensitive. If you leave the connector list blank, this script returns data for all connectors. You cannot enter a single letter to get data for all connectors starting with that letter. You must enter the exact name of the connector. It may be easier to leave this parameter blank and check the data detail for the connectors of interest.
Start date	Specify a start date for beginning the message count. Use the YYYY/MM/DD format.
End date	Specify an end date for beginning the message count. Use the YYYY/MM/DD format.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

MsgsThroughSMTPService

Use this Knowledge Script to monitor the size and number of messages through the SMTP Service for the specified days. You can specify the interval to be a number of past days or start and stop dates.

Either interval specification looks at entries in the message tracking logs for the indicated days. If *Past N days to average messages* is 1, it looks at all the entries in today's log, since midnight, when it started, regardless of what time of day it is now. If *Past N days to average messages* is 2 it also examines the log from the day before that (all 24 hours of it).

Tracking logs are implemented using the network share `<servername>.log`. This shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of SMTP messages sent and received. The default is n.
Maximum threshold for number of received mail messages	Specify the maximum number of SMTP messages that can be received before an event is raised. The default is 300.
Maximum threshold for number of sent mail messages	Specify the maximum number of SMTP messages that can be sent before an event is raised. The default is 300.
Include Exchange system messages?	Set to **y** to include Exchange system messages. The default option is n.
Past N days to average messages	Specify the number of days over which to monitor SMTP messages. This value is ignored if you specify start and end dates. The default value is 3 days.
Start date (YYYY/MM/DD)	Specify the start date for monitoring SMTP messages.
End date (YYYY/MM/DD)	Specify the end date for monitoring SMTP messages.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

MsgsThruSMTPSvcByInterval

Use this Knowledge Script to monitor the size and number of messages through the SMTP Service during the monitoring interval. The monitoring interval is since the last time the script ran.

Tracking logs are implemented using the network share `<servername>.log`. This shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of SMTP messages sent and received. The default is n.
Maximum threshold for number of received mail messages	Specify the maximum number of SMTP messages that can be received before an event is raised. The default is 300.
Maximum threshold for number of sent mail messages	Specify the maximum number of SMTP messages that can be sent before an event is raised. The default is 300.
Include Exchange system messages?	Set to **y** to include Exchange system messages. The default is n.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

MsgsWithinAdminGroup

Use this Knowledge Script to monitor the total number and size of messages transferred between Exchange servers in the same Admin Group during the specified number of days or from a specific start date to a specific end date.

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log`. This shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Note
Daily Exchange server logs begin and end at midnight using Coordinated Universal Time (UTC) rather than local time. The UTC standard is equivalent to Greenwich Mean Time (GMT). This script also uses GMT and does not adjust for your time zone. Depending on your time zone, the number of days (in local time) may not represent the corresponding number of GMT hours. For example, if you monitor the previous day's messages (Count messages from past N days is set to 1), and your time zone is GMT -08:00 (Pacific Time), running the Knowledge Script job at 09:00 will monitor only 16 hours of the day's Exchange server log recorded in GMT. If your time zone is GMT, your results will be accurate.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event when a threshold is exceeded. The default option is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of received and sent messages. The default is n.
Maximum threshold for number of received messages	Specify the maximum number of messages that can be received from other Exchange servers within the Admin Group before an event is raised. The default is 300 messages.
Maximum threshold for number of sent messages	Specify the maximum number of messages that can be sent from this Exchange server to other Exchange servers in the same Admin Group before an event is raised. The default is 300 messages.
Include Exchange system messages?	Set to **y** to include system messages in the message count. The default option is n.
Count messages from past N days	Specify the number of previous days (including today) to track back for the message count. For example, to find the number of messages transferred in the past week, enter 7. The default value is 3 days. If you set a start and end date, the number of previous days parameter is ignored.

Description	How to Set It
Start date (YYYY/MM/DD)	Specify a start date for beginning the message count.
End date (YYYY/MM/DD)	Specify an end date for stopping the message count.
Refresh server info at each interval?	Set to **y** to generate a table showing the Exchange 2000 or Exchange Server 2003 servers and the admin groups to which they belong. In large organizations with hundred of servers, creating this table may take a while. Therefore, this parameter allows you to decide whether to create the table every time the script runs. If the customer environment is pretty static, there is little need to create the table. On the other hand, if the customer environment is very dynamic and the servers are frequently moved across different admin groups, then it is preferable to set this parameter to **y**. The default is n.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

MsgsWthnAdmnGrpByInterval

Use this Knowledge Script to monitor the total number and size of messages sent and received between Exchange servers in the same Admin Group since last time the Knowledge Script ran (a delta value).

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log`. This shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share.

This script reports 0 messages transferred if you delete the tracking logs or do not enable them.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event when a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the following data collected during the monitoring interval: • Size (KB) of messages sent within this Admin Group • Number of messages sent within this Admin Group • Size (KB) of messages received within this Admin Group • Number of messages received within this Admin Group The default is n.
Maximum threshold for number of received messages	Specify the maximum number of messages that can be received by this server from other Exchange servers within this Admin Group before an event is raised. The default is 300 messages.
Maximum threshold for number of sent messages	Specify the maximum number of messages that can be sent from other Exchange servers within this Admin Group to this server before an event is raised. The default is 300 messages.
Include Exchange system messages?	Set to **y** to include system messages in the message count. The default is n.
Refresh server info at each interval?	Set to **y** to generate a table showing the Exchange servers and the Admin Groups to which they belong. In large organizations with hundred of servers, creating this table may take a while. Therefore, this parameter allows you to decide whether to create the table every time the script runs. If your environment is pretty static, there is little need to create the table. On the other hand, if your environment is very dynamic and the servers are moved frequently across different Admin Groups, then it is preferable to set this parameter to **y**. The default is n.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which the number of received or sent messages exceeds the threshold. The default is 5 (red event indicator).

MTAConnectionQueueLength

Use this Knowledge Script to monitor the queue length of all message transfer agent (MTA) connections, including the MTAs to other servers in the site, public and private information stores, and any installed connectors (such as X.400 Connectors). If the server is a replication bridgehead, the MTA will also have a queue to the directory on its server.

You specify the maximum number of queued inbound and outbound messages, the maximum number of queued recipients, and the number of consecutive times the threshold can be exceeded before raising an event. This script raises an event if the number of queued inbound messages, queued outbound messages, or queued recipients exceeds the threshold you set.

Resource Object

Information Store folder

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the queue length for an MTA connection exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the queue length for each MTA connection. The default is n.
Maximum threshold for number of inbound messages	Specify the maximum number of inbound messages that can be queued before an event is raised. The default is 10000 messages.
Maximum threshold for number of outbound messages	Specify the maximum number of outbound messages that can be queued before an event is raised. The default is 10000 messages.
Maximum threshold for total number of messages	Specify the maximum total number of messages that can be queued before an event is raised The default is 100 messages.
Maximum threshold for number queued recipients	Specify the maximum number of recipients that can be queued before an event is raised. The default is 100 recipients.
List of MTA connection queues to monitor	Provide the names of the MTA connection queues to monitor (case-sensitive) in a comma-separated list or specify **ALL** to monitor all MTA connection queues. The default is ALL.

Description	How to Set It
Consecutive number of times before an event	Specify the consecutive number of intervals the threshold for queued messages or recipients can be exceeded before the Knowledge Script raises an event. The default is 5 consecutive intervals. Because queued messages or queued recipients can have periodic spikes, you may want to set this parameter to a higher value to filter out unnecessary events. For example, you may want to allow the number of queued messages to exceed the threshold 3 to 4 times before you are alerted.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

NNTPConnections

Use this Knowledge Script to monitor the total number of inbound and outbound connections to the Network News Transfer Protocol (NNTP) service. This script raises an event if the number of connections exceeds the threshold you set.

Resource Object

NNTP Virtual Server

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • Total connections • Current connections • Total SSL connections • Total outbound connections The default is n.
Maximum threshold for total number of NNTP connections	Specify the maximum number of inbound and outbound NNTP connections that can have occurred since the server was last started. This script raises an event if the number of connections exceeds this threshold. The default is 500 connections.
Maximum threshold for number of outbound NNTP connections	Specify the maximum number of outbound NNTP connections that can have occurred since the NNTP server was last started. This script raises an event if the number of connections exceeds this threshold. The default is 1000 connections.
Maximum threshold for number of current NNTP connections	Specify the maximum number of concurrent NNTP connections that can occur before an event is raised. The default is 100 connections.
Maximum threshold for number of SSL connections	Specify the maximum number of SSL connections that can occur before an event is raised. The default is 1000 connections.
Consecutive number of times before an event	Specify the maximum number of consecutive times that each connection threshold can be exceeded before an event is raised. For example, if this parameter is set to 3 and the number of SSL connections exceeds the threshold each time the job runs, this script raises an event the third time the job runs. The default is 5 consecutive occurrences.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

NumberOfMailboxes

Use this Knowledge Script to monitor the total number of Exchange mailboxes. This script raises an event if the number of mailboxes exceeds the threshold you set.

On a computer with more than one virtual server, the total number of mailboxes is calculated as the total number of mailboxes for all virtual servers on the computer.

If a failover occurs when this script job is running, the job restarts on the new node. It is normal for the job on the failed node to generate one or more error messages, depending on what it was doing when the failover occurred.

Note
This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of mailboxes on the Exchange server exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of mailboxes found. The default is n.
Maximum threshold for number of mailboxes	Specify the maximum number of mailboxes that can be on an Exchange server before an event is raised. The default is 300 mailboxes.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.

Description	How to Set It
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mailbox alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of mailboxes exceeds the threshold. The default is 5 (red event indicator).

PFAclChanges

This Knowledge Script checks for changes in the access control lists for each folder in the public information store. This script raises an event if the script cannot collect information for a public folder.

Note
This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of access control list changes exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of changes to a public folder's access control list. The default is n.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Maximum threshold for number of ACL changes	Specify the maximum number of changes to the public folder's access control list that can occur before an event is raised. The default is 0 (zero).
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default value is 5 (red event indicator).

PFAclInfo

This Knowledge Script collects data about the access control list for each folder in the public information store. This script raises an event if the script cannot collect data about a public information store.

Note
This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which data cannot be collected. The default is 5 (red event indicator).

PFInfo

This Knowledge Script monitors the number and size of public folders, and the number of messages in the public folders. You can set the data collection level to configure the level of collected public folder data. For more information, see "Setting the Level of Data Collection" on page 113.

Note
This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of public folders, the total size of all public folders, or the number of messages in all public folders exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the following information, depending on the level of data detail you specify: • Number of public folders • Total size for all public folders (KB) • Number of messages stored in public folders For more information, see "Setting the Level of Data Collection" on page 113. The default is n.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Maximum threshold for number of public folders	Specify the maximum number of public folders that can exist before an event is raised. The default is 100 public folders.

Description	How to Set It
Maximum threshold for size of file space (MB)	Specify the maximum size public folders can attain before an event is raised. The default is 300 MB.
Maximum threshold for number of messages	Specify the maximum number of messages that public folders can contain before an event is raised. The default is 30000 messages.
Character to separate data detail columns	Provide a character to use to separate the columns in the detail data. The default character is "|". If you change this parameter to Null, a Tab character is specified.
Detail level (1-3) for data collection	Specify a value (1, 2, or 3) to specify the level of data collection. The default value is 3. For more information, see "Setting the Level of Data Collection" on page 113.
Range of message size	Monitor the number of messages in a range of sizes by specifying each size range in a comma-separated list. Specify the message size in kilobytes (KB). For example, if you enter "100,500,1000", this script returns the number of messages that are: • Less than 100 KB • Between 100 KB and 500 KB • Between 500 KB and 1000 KB • Greater than 1000 KB The default is "100,500,1000,2000".
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

Setting the Level of Data Collection

If you set the *Detail level (1-3) for data collection* parameter to **1**, the script returns the following information:

- Name of the public folder
- Size of messages in the public folder
- Number of messages in the public folder
- Path of the public folder
- Creation time of the public folder
- Last modification time of the public folder
- Last access time of the public folder
- Number of attachments in the public folder
- Number of messages in the public folder which have attachments
- Number of owners of the public folder

If you set the *Detail level (1-3) for data collection* parameter to **2**, the script returns the all of the information in level 1, plus the following additional information:

- Oldest message creation time
- Oldest message modification time
- Newest message creation time
- Newest message modification time

If you set the **Detail level (1-3) for data collection** to **3**, the script returns the all of the information in levels 1 and 2, plus the number of messages in user-defined size ranges. For example, the number of messages that are between one and ten KB.

PFReplicationByObj

This Knowledge Script monitors public folder replication between Exchange servers by updating a test object on a local public folder and checking the replica folder on one or more remote Exchange servers for the replicated object.

Before you run this script:

- Create a public folder on the local Exchange server for creating and updating the test object.
- Configure this public folder to be hosted by the remote Exchange servers you want to test.

Note

This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of unreplicated test objects on a remote Exchange server exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the replication status of the test object on each remote Exchange server. The default is n.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.

Description	How to Set It

List of remote servers to host test object	Specify a list of remote Exchange servers that host a replica of the test object on the local Exchange server. Use the following syntax:
	`<computer>(/O=<organization>/OU=<administrative group>`
	Where:
	• ***computer*** specifies the name of the computer on which the Exchange server is installed
	• ***organization*** specifies the name of the Exchange organization to which the server belongs
	• ***administrative group*** specifies the name of the Exchange administrative group to which the server belongs
	Separate more than one server name using "|", for example:
	`Server1(/O=Org1/OU=AdminGrp1)|Server2(/O=Org2/OU=AdminGrp2)`

Local public folder to maintain test object	Specify the name of the local public folder that the Knowledge Script uses to create and update the test object. The folder name must start with "\". For example, to specify a public folder named "aaa", enter "\aaa". The default is "\".
Maximum threshold for number of unreplicated changes	Specify the maximum number of unreplicated changes that can occur between the local public folder and a public folder on a remote Exchange server. This script raises an event if the number of unreplicated changes exceeds the threshold. The default is 5 unreplicated changes.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of unreplicated changes exceeds the threshold. The default is 5 (red event indicator).

POP3Accesses

Use this Knowledge Script to monitor the number of POP3 access operations. The POP3 access operations include `LAST`, `STAT`, `LIST`, `DEL`, `NOOP`, and `RSET` operations. This script raises an event if the total number of POP3 access operations exceeds the threshold you set.

Resource Object

POP3 Virtual Server

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of POP3 access operations exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled data collection returns the number of POP3 access operations. The default is n.
Maximum threshold for number of POP3 access operations	Specify the maximum number of POP3 access operations that can occur before an event is raised. The default is 10000 access operations.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

POP3Authenticate

Use this Knowledge Script to monitor the authentication of POP3 protocols. This script raises an event if the rate of failure of total authentications exceeds the threshold.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003, Protocols folder

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of authentication failures exceeds the threshold you set. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • Number of authenticate commands received since startup • Number of authenticate commands per second • Number of authenticate command failures since startup The default is n.
Maximum threshold for number of authentication failures	Specify the maximum number of authentication failures that can have occurred since startup. This script raises an event if the number of failures exceeds this threshold. The default is 1000.
Consecutive number of times before an event	Specify the maximum number of consecutive times the threshold can be exceeded before this script raises an event. The default is 5 consecutive occurrences.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

POP3Connections

Use this Knowledge Script to monitor the number of current and total connections to the POP3 service. You specify the maximum number of current and total connections and the number of consecutive times the threshold can be exceeded before raising an event. This script raises an event if the current or the total connections exceed the threshold for the specified consecutive number of intervals.

Resource Object

POP3 Virtual Server

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns: • Total connections • Current connections The default is n.
Maximum threshold for total number of connections	Specify the maximum number of POP3 connections that can have occurred since the POP3 server was last started. This script raises an event if the number of connections exceeds this threshold. The default is 1000 connections.
Maximum threshold for number of current POP3 connections	Specify the maximum number of POP3 connections that can occur during the current monitoring interval. This script raises an event if the number of connections exceeds the threshold. The default is 100 connections.
Consecutive number of times before an event	Specify the consecutive number of intervals the threshold for connections can be exceeded before raising an event. The default is 5 consecutive intervals. Because connections can have periodic spikes, you can set this parameter to a higher value to filter out unnecessary events. For example, you can allow the number of current connections to exceed the threshold 3 to 4 times before an event is raised.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ProtocolVSStatus

Use this Knowledge Script to monitor the status of HTTP, NNTP, POP3, IMAP4, and SMTP virtual servers. This script attempts to restart a virtual server that is detected as down.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Automatically restart service?	Set to **y** to automatically restart a service that is down. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns 100 if a monitored virtual server is up, 0 if a monitored virtual server is down. The default is n.
Event?	Set to **y** to raise an event if a service is down and restart fails or succeeds, or you do not want to restart. The default is y.
Severity: Failed to restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and AppManager fails to restart the service. The default is 5 (red event indicator).
Severity: Successful restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and AppManager successfully restarts the service. The default is 25 (blue event indicator).
Severity: Do not restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and you do not want AppManager to restart the service. The default value is 18 (yellow event indicator).

PublicStoreMountStatus

Use this Knowledge Script to monitor the mount status of one or more public stores. When a public store is unmounted, the Exchange Server cannot store information in it or read information from it.

Resource Object

Information Store folder, Public Store object

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a public store is unmounted. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns 100 if the public store is mounted, 0 if the public folder store is unmounted. The default is n.
Event severity	Set the event notification level, from 1 to 40, to indicate the importance of an event in which a public store is unmounted. The default is 5 (red event indicator).

QueueStatus

Use this Knowledge Script to monitor the inbound and outbound message queue status of all X.400 and SMTP virtual servers, including the number, size, and elapsed time for messages that reside in a message queue. This script raises an event if the number, size, or elapsed time exceeds the threshold you set.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Once a day**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Specify a protocol (X400, SMTP, or ALL)	Select one of the following to specify the protocols to monitor (not case-sensitive): • **X400** monitors the X.400 protocol. • **SMTP** monitors the SMTP protocol. • **ALL** monitors both X.400 and SMTP protocols. The default is ALL.
Collect total number of messages, queue sizes and elapsed time of queues?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the total number of messages, queue size, and elapsed time of inbound and outbound message queues. The default is n.
Collect data for number of messages in queues?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of messages in a message queue. The default is n.
Threshold - Maximum for number of messages in queues	Specify the maximum number of messages that can be in a queue before an event is raised. The default is 1000.
Event for number of messages in queues?	Set to **y** to raise an event when the number of messages in queue exceeds the threshold. The default is y.
Event severity: Number of messages in queues	Set the event severity level, from 1 to 40, to specify the importance of an event in which the number of messages in queue exceeds the threshold. The default is 5.
Collect data for size of queues?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the size of a message queue. The default is n.
Threshold - Maximum for size of queues	Specify the maximum size a queue can attain before an event is raised. The default is 100 MB.
Event for size of queues?	Set to **y** to raise an event when the size of a message queue exceeds the threshold. The default is y.
Event severity: Size of queues	Set the event severity level, from 1 to 40, to specify the importance of an event in which the size of a message queue exceeds the threshold. The default is 5.
Collect data for elapsed time in queues?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the oldest messages in a message queue. The default is n.

Description	How to Set It
Threshold - Maximum for elapsed time in queues	Specify the maximum number of seconds a message can remain in queue before an event is raised. The default is 1000.
Event for elapsed time in queues?	Set to **y** to raise an event when a message spends too long in a queue. The default is y.
Event severity: Elapsed time in queues	Set the event severity level, from 1 to 40, to specify the importance of an event in which a message spends too long in a queue. The default is 5.

Report_Connectivity

Use this Knowledge Script to generate a report about the connectivity between Exchange 2000 Server and Exchange Server 2003. This report uses data collected by the Connectivity Knowledge Script.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

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.
Data settings	
Hours or percentage on chart	Select whether to illustrate availability by **Hours** or by **Percentage**.
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom N or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Report settings	
Include parameter help card?	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 yes.
Select chart style	Click **Browse [...]** to define the graphic properties of the charts in your report.
Select output folder	Click **Browse [...]** to set parameters for the output folder.

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. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Click **Browse [...]** to set the report properties as desired.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event 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 level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a report contains no data. The default is 25 (blue level indicator).
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_ISPrivateResourceSummary

Use this Knowledge Script to generate a report about the file space used by private information store folders and mailboxes. This report allows you to make a statistical analysis of the data point values over the time range you define for the report. This report uses data collected by the TopNISMailboxRes Knowledge Script.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

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.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time range of the report • **Minimum**: The minimum value of data points for the time range of the report • **Maximum**: The maximum value of data points for the time range of the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time range of the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the time range of the report • **Close**: The last value for the time range of the report • **Change**: The difference between the first and last values for the time range of the report (close - open = change) • **Count**: The number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/ bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom N or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	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 yes.
Select chart style	Click **Browse [...]** to define the graphic properties of the charts in your report.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Click **Browse [...]** to set the report properties as desired.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event 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 level indicator).

Description	How to Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25 (blue level indicator).
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_ISPublicResourceSummary

Use this Knowledge Script to generate a report about the file space used by public information store folders. This report allows you to make a statistical analysis of the data point values over the time range you define for the report. This report uses data collected by the TopNISPublicRes Knowledge Script.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

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.
Select the style	Select the style for the report: • **By computer** shows one value for each computer you selected. • **By legend** shows one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console). • **By computer and legend** shows one value for each unique legend from each computer.
Data settings	
Statistics to show	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the time range of the report • **Minimum**: The minimum value of data points for the time range of the report • **Maximum**: The maximum value of data points for the time range of the report • **Min/Avg/Max**: The minimum, average, and maximum values of data points for the time range of the report • **Range**: The range of values in the data stream (maximum - minimum = range) • **StandardDeviation**: The measure of how widely values are dispersed from the mean • **Sum**: The total value of data points for the time range of the report • **Close**: The last value for the time range of the report • **Change**: The difference between the first and last values for the time range of the report (close - open = change) • **Count**: The number of data points for the time range of the report

Description	How to Set It
Select sorting/display option	Select whether data is sorted, or the method of display: • **No sort**: Data is not sorted • **Sort**: Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right) • **Top %**: Chart only the top N % of selected data (sorted by default) • **Top N**: Chart only the top N of selected data (sorted by default) • **Bottom %**: Chart only the bottom N % of data (sorted by default) • **Bottom N**: Chart only the bottom N of selected data (sorted by default)
Percentage/count for top/ bottom	Specify a number for either the percent or count defined in the previous parameter (for example, Top 10%, or Top 10). The default is 25.
Truncate top/bottom?	If set to **yes**, then the data table shows only the top or bottom N or % (for example, only the top 10%). Otherwise, the table shows all data. The default is no.
Show totals on the table?	If set to **yes**, then additional calculations are made for each column of numbers in a table, and the following values are listed at the end of the table: • **Report Average**: An average of all values in a column • **Report Minimum**: The minimum value in a column • **Report Maximum**: The maximum value in a column • **Report Total**: The total of all values in a column The default is no.
Report settings	
Include parameter help card?	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 yes.
Select chart style	Click **Browse [...]** to define the graphic properties of the charts in your report.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Click **Browse [...]** to set the report properties as desired.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event 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 level indicator).

Description	How to Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25 (blue level indicator).
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_ServerLoad

Use this Knowledge Script to generate a report about the rate at which the Exchange server sends and receives messages and the rate at which the Exchange server processes the RPC packets. This report lets you aggregate the data by time period (minute, hour, or day) and calculate statistics for each period (for example, the average value per hour).

This report uses data collected by the ServerLoad Knowledge Script.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

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 the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (For example, each page shows the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
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.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval (for example, the average value for 1 Hour) • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	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 yes.
Select chart style	Click **Browse [...]** to define the graphic properties of the charts in your report.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Click **Browse [...]** to set report properties as desired.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event 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 level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25 (blue level indicator).
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_ServerMessage

Use this Knowledge Script to generate a report about the total number of mail recipients, messages delivered, messages sent, messages submitted, the mailbox store, and the public information store. This report lets you aggregate the data by time period (minute, hour, or day) and calculate statistics for each period (for example, the average value per hour).

This report uses data collected by the ServerTotalMsg Knowledge Script.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

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 the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (For example, each page shows the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
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.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval (for example, the average value for 1 Hour) • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	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 yes.
Select chart style	Click **Browse [...]** to define the graphic properties of the charts in your report.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Click **Browse [...]** to set report parameters as desired.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event 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 level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25 (blue level indicator).
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_ServerUsers

Use this Knowledge Script to generate a report about the number of users connected to the information store. This report lets you aggregate the data by time period (minute, hour, or day) and calculate statistics for each period (for example, the average value per hour).

This report uses data collected by the ServerUsers Knowledge Script.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

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 the style	Select the style for the first page of the report: • **By computer** provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer) • **By data stream** provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (For example, each page shows the value of the *NT_CpuResource-All Threads(#)* data stream from each computer) • **By computer and data stream** provides links to pages showing a single data stream collected from a computer • **All data streams on one page** generates a report with all data on a single page
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.
Aggregation by	Select the aggregation method for the data in your report: • Minute • Hour • Day
Aggregation interval	Select the interval by which the data in your report is aggregated. Possible values range from 1 to 90.

Description	How to Set It
Statistics to show per period	Select a statistical method by which to display data in the report: • **Average**: The average value of data points for the aggregation interval (for example, the average value for 1 Hour) • **Minimum**: The minimum value of data points for the aggregation interval • **Maximum**: The maximum value of data points for the aggregation interval • **Count**: The number of data points for the aggregation interval • **Sum**: The total value of data points for the aggregation interval • **3Sigma**: The average + (3 * standard deviation) and average - (3 * standard deviation) • **Std**: The standard deviation • **Box**: Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval • **Open**: The first value for the aggregation interval • **Close**: the last value for the aggregation interval
Report settings	
Include parameter help card?	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 yes.
Select chart style	Click **Browse [...]** to define the graphic properties of the charts in your report.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Click **Browse [...]** to set report parameters as desired.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event 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 level indicator).
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25 (blue level indicator).
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_TopNMailboxesInfo

Use this Knowledge Script to generate a report about the file space (in MB) used by the top private information store folders or mailboxes.

This report uses data collected by the TopNISMailboxRes Knowledge Script.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

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.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Click **Browse [...]** to set report properties as desired.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event 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 level indicator).

Description	How to Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25 (blue level indicator).
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_TopNReceivers

Use this Knowledge Script to generate a report about which users received the most mail messages, and the total file size of messages received by the top users or by all users.

This report uses data collected by the TopNReceivers Knowledge Script.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

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.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Select properties	Click **Browse [...]** to set report properties as desired.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event 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 level indicator).

Description	How to Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25 (blue level indicator).
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

Report_TopNSenders

Use this Knowledge Script to generate a report about which users sent the most mail messages, and the total file size of messages sent by the top users or by all users.

This report uses data collected by the TopNSenders Knowledge Script.

Resource Object

Report Agent

Default Schedule

The default schedule is **Run once**.

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.
Report settings	
Include parameter help card?	Set to **yes** to include a table in the report that lists parameter settings for the report script. The default is yes.
Select output folder	Click **Browse [...]** to set parameters for the output folder.
Select properties	Click **Browse [...]** to set the properties parameters as desired.
Add job ID to output folder name?	Set to **yes** to append the job ID to the name of the output folder. A job ID helps you correlate a specific instance of a Report Script with the corresponding report. The default is no.
Add time stamp to title?	Set to **yes** to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. A time stamp lets you run consecutive iterations of the same report without overwriting previous output. The default is no.
Event notification	
Event for report success?	Set to **yes** to raise an event when the report is successfully generated. The default is yes.
Severity level for report success	Set the event 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 level indicator).

Description	How to Set It
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25 (blue level indicator).
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the report is not generated. The default is 5 (red level indicator).

ResponseTime

Use this Knowledge Script to check the mail response time between two or more Exchange 2000 servers or Exchange Server 2003 servers. This script cannot monitor more than one Exchange 2000 or Exchange Server 2003 virtual server.

If you only have one Exchange server, do not use this script. If you only have one Exchange server, this script incorrectly reports that the Exchange Server is down. To monitor response time for a single Exchange server, use the AppManager ResponseTime for Microsoft Exchange module.

This script determines if e-mail is delivered and the time it takes for the message to be delivered. In addition, this script raises an event if a reply to the test message is not received within the response time threshold you set.

To run this script on a group of Exchange servers, each server must have the same profile name.

If a failover occurs when this script job is running, the job restarts on the new node. It is normal for the job on the failed node to generate one or more error messages, depending on what it was doing when the failover occurred.

Note

This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 15 minutes**, which is appropriate if you are monitoring Exchange servers in a connected network.

If your Exchange servers rely on a remote WAN or LAN service (such as RAS) or a dial-up modem that is not always connected, you can set up server group folders to separate Exchange servers into different groups. Then you can set the schedule interval for this script to run on each folder based on each group's connection schedule.

For example, you can create one server group for your always-connected servers and a separate folder for offhours RAS connections and create two different sets of jobs with different schedules (frequently for your connected network and once a day or based on the scheduled connection time for the remote access servers). For information about setting up server groups, see the *User Guide for AppManager*.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the response time threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the response time in seconds for each Exchange server. The default is y.
Exchange profile for NetIQmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager. This is especially true if you are running this script on the top-level Exchange folder or Exchange server groups.
Mailbox alias for NetIQmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager. This is especially true if you are running this script on the top-level Exchange folder or Exchange server groups.
Maximum threshold for response (in seconds)	Specify the maximum number of seconds that can elapse from the time the test message is sent out until a reply should be received. The default response time is 120 seconds.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event which the response time threshold is exceeded. The default value is 5 (red event indicator).

Example of How This Script is Used

To measure response time, this Knowledge Script sends a test mail message to each of Exchange servers being tested, using the profile and mailbox alias name set up for the computer running the job using AppManager Security Manager or the parameters specified in this script. After the test message is delivered by the "sending" server, each of the "receiving" servers responds with a reply. The response time is the time it takes for the "sending" server to receive this reply from the mail recipient.

For example, assume you run this script on a server group folder with the Exchange servers Paris, Cabernet, Dynamo, Boston, and Nero. The **netiq-Paris** Exchange client on Paris sends a message to Cabernet, Dynamo, Boston, and Nero. If Cabernet **(netiq-Cabernet)** responds and Paris receives the reply 60 seconds later, the response time from Paris to Cabernet is 60 seconds.

Simultaneously, the **netiq-Cabernet** Exchange client on Cabernet is sending test messages to Paris, Dynamo, Boston, and Nero. If the reply from Paris **(netiq-Paris)** is received 90 seconds after delivery, then the response time from Cabernet to Paris is 90 seconds.

Although this example focuses on the communication and response time between Paris and Cabernet, the same send-and-reply operations are taking place for all of the servers in the group.

Locale Considerations

This Knowledge Script asks Exchange to send a delivery-receipt message when the test e-mail is delivered to the recipient. In the English version of AppManager, this script looks for a delivery-receipt e-mail whose subject line is "Delivered."

If the recipient uses an Exchange server configured with a different locale, the subject line of the response is the word "Delivered" translated into that locale's language.

The English version of AppManager does not recognize a non-English response and, likewise, the Japanese version of AppManager does not recognize a non-Japanese response.

ServerHealth

Use this Knowledge Script to monitor the health of the Exchange server. This script monitors the percentage of time that all processors on the Exchange server are busy and the percentage of elapsed time that the Exchange server process threads are used to execute instructions. In addition, this script raises an event if a monitored value exceeds the threshold you set.

This script tracks the following performance objects:

Object	Counter	Instance
Processor	% Processor Time	_Total
Process	% Processor Time	inetinfo
Process	% Processor Time	EMSMTA
Process	% Processor Time	STORE
Process	% Processor Time	MAD
Memory	Pages/sec	

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns either the current value or the delta value for each monitored performance counter. The default is n.
Compare to previous monitoring interval?	Set to **y** to compare the data collected in the current monitoring interval to the previous monitoring interval. If set to y, any graphs you create plot the comparison value rather than the total value. If set to y, the data collected and the thresholds you set can be positive or negative. The default is n.
Maximum threshold for total processor usage	Specify the maximum percentage of time that all the processors on the system can be busy executing non-idle threads. This value can be viewed as the fraction of the time spent doing useful work. On a multi-processor system, if all processors are always busy this is 100%, if all processors are 50% busy this is 50% and if 25%of the processors are 100% busy, this is 25%. The default is 99%.
Maximum threshold for processor usage by Exchange services	Specify the maximum percentage of elapsed processor time that all of the threads the Exchange server processes can use to execute instructions. Code executed to handle certain hardware interrupts or trap conditions may be counted. The default is 10%.

Description	How to Set It
Maximum threshold for total memory pages per second	Specify the maximum number of pages that can be read from the disk or written to the disk to resolve memory references. This value is the sum of pages input/sec and pages output/sec and includes paging traffic on behalf of the system Cache to access file data for applications and pages to and from non-cached, mapped memory files. The default is 200 memory pages per second. **Tip** This is the primary counter to observe if you are concerned about excessive memory pressure (thrashing), and the excessive paging that may result.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ServerHistory

Use this Knowledge Script to monitor the complete message history for an Exchange server. This script monitors the combined message count for the mailbox stores and public information stores.

This script raises an event if the number of messages exceeds the threshold you set.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the following data: • Number of recipients that have received a message (message recipients delivered - private information or mailbox store). • Number of messages delivered (messages delivered - private information or mailbox store). • Number of messages sent (messages sent - private information or mailbox store). • Number of messages submitted (messages submitted - public information store). • Number of recipients that have received messages (message recipients delivered - public information store). • Number of messages sent (messages sent - public information store). • Number of Exchange users • MTA work queue length. The default is n.

Description	How to Set It
Maximum threshold for number of messages	Specify the total number of messages that can have occurred since startup before an event is raised. The default is 10000 messages. To track messages, this script monitors the following: Mailbox information store: • Total number of recipients that have received a message since startup (message recipients delivered). • Total number of messages delivered to all recipients since startup (messages delivered). • Total number of messages sent to other storage providers via Message Transfer Agent (MTA) since startup (messages sent). • Total number of messages submitted by clients since startup (messages submitted). Public information store: • Total number of recipients that have received a message since startup (message recipients delivered). • Total number of messages sent to other storage providers via MTA since startup (messages sent).
Maximum threshold for number of users	Specify the maximum number of users that can be connected to the private and public information store or mailbox store and public information store before an event is raised. The default is 500 users.
Maximum threshold for number of messages in work queue	Specify the maximum number of outstanding messages that can be in the work queue before an event is raised. Messages in the work queue have not yet been processed to completion by the MTA. The default is 5 messages.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ServerLoad

Use this Knowledge Script to monitor the load on the Exchange server. This script tracks the rate at which the Exchange server receives and submits messages per minute. This script also monitors the rate at which the Exchange server processes the RPC packets. This script raises an event if a threshold is exceeded.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the following load information: • Rate of messages delivered per minute • Rate of messages submitted per minute • Rate of delivery for RPC packets per second **Note** The specific data streams you see will depend on the version of Exchange you are monitoring. The default is n.
Threshold for delivered private messages per minute	Specify the maximum rate at which recipients can receive private messages before an event is raised. The default is 500 per minute.
Threshold for submitted private messages per minute	Specify the maximum rate at which private messages can be submitted by clients before an event is raised. The default is 500 per minute.
Threshold for delivered public messages per minute	Specify the maximum rate at which recipients can receive public messages before an event is raised. The default is 500 per minute.
Threshold for submitted public messages per minute	Specify the maximum rate at which public messages can be submitted by clients before an event is raised. The default is 500 per minute.
Threshold for adjacent MTA associations	Specify the maximum number of open associations that this MTA can have to other MTAs before an event raised. The default is 100.
Threshold for processed RPC packets per second	Specify the maximum rate at which RPC packets can be processed before an event is raised. The default is 500 per second.
Threshold for address book browse operations per second	Specify the maximum rate at which address book clients can perform browse operation before an event is raised. The default is 150 per second.
Threshold for address book read operations per second	Specify the maximum rate at which address book clients can perform read operations before an event is raised. The default is 100 per second.

Description	How to Set It
Threshold for extended directory service read operations per second	Specify the maximum rate at which extended directory service clients can perform read operations before an event is raised. The default is 50 per second.
Threshold for directory service replication updates per second	Specify the maximum rate at which replication updates can be applied by the local directory service before an event is raised. The replication rate indicates how much replication activity is occurring on the server. The default is 50 per second.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ServerQueues

Use this Knowledge Script to monitor Exchange server queues, including the MTA work queue and the IS Private and IS Public send and receive queues. This script raises an event if a queue exceeds the threshold you set.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 30 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the queue length for each queue monitored. The default is n.
Threshold for number of messages in MTA work queue	Specify the maximum number of outstanding messages that can be in the work queue before an event is raised. The work queue contains messages not yet processed to completion by the MTA. The default is 20 messages.
Threshold for number of private messages in send queue	Specify the maximum number of private messages that can be in the send queue before an event is raised. The default is 20 messages.
Threshold for number of public messages in send queue	Specify the maximum number of public messages that can be in the send queue before an event is raised. The default is 20 messages.
Threshold for number of private messages in receive queue	Specify the maximum number of private messages that can be in the receive queue before an event is raised. The default is 20 messages.
Threshold for number of public messages in receive queue	Specify the maximum number of public messages that can be in the receive queue before an event is raised. The default is 20 messages.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ServerTotalMsg

Use this Knowledge Script to monitor the total number of messages for an Exchange server. You can set separate thresholds for the total number of mail recipients, the number of messages delivered, the number of messages sent, the number of messages submitted, and the number of messages waiting to be delivered for the mailbox store and public information store. This script raises an event if the server exceeds a threshold.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the following information: • Number of recipients to whom messages were delivered • Number of messages delivered • Number of messages sent • Number of messages submitted • Number of messages still outstanding The default is n.
Maximum threshold for private message recipients	Specify the maximum number of recipients that can receive private messages before an event is raised. The default is 800.
Maximum threshold for private delivered messages	Specify the maximum number of private messages that can be delivered to all recipients before an event is raised. The default is 800. This parameter is applicable for the mailbox store on Exchange 2000 Server.
Maximum threshold for private sent messages	Specify the maximum number of private messages that can be sent to other storage providers by Message Transfer Agent (MTA). This script raises an event if the number of messages exceeds the threshold. The default is 800. This parameter is applicable for the mailbox store on Exchange 2000 Server.
Maximum threshold for private submitted messages	Specify the maximum number of private messages that can be submitted by clients before an event is raised. The default is 800. This parameter is applicable for the mailbox store on Exchange 2000 Server.

Description	How to Set It
Maximum threshold for private outstanding messages	Specify the maximum number of private messages that can be waiting for delivery before an event is raised. The default is 800. This parameter is applicable for the mailbox store on Exchange 2000 Server.
Maximum threshold for public message recipients	Specify the maximum number of recipients that can receive public messages before an event is raised. The default is 800.
Maximum threshold for public sent messages	Specify the maximum number of public messages that can be sent to other storage providers by Message Transfer Agent (MTA). This script raises an event if the number of messages exceeds the threshold. The default is 800.
Maximum threshold for public submitted messages	Specify the maximum number of public messages that can be submitted before an event is raised. The default is 800.
Maximum threshold for public outstanding messages	Specify the maximum number of public messages that can be waiting for delivery before an event is raised. The default is 800.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

ServerUsers

Use this Knowledge Script to monitor the number of users connected to the information store. This script raises an event if the number of users exceeds the threshold you set.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every hour**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if the number of user connections exceeds the threshold. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of user connections. The default is n.
Maximum threshold for number of connected users	Specify the maximum number of users that can be connected to the information store before an event is raised. The default is 500 users.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of user connections exceeds the threshold. The default is 5 (red event indicator).

ServicesDown

Use this Knowledge Script to monitor the up and down status of Exchange services. This script checks services using the known order of dependency, which is managed by the Windows service controller. If any service is detected as down, this script can automatically attempt to restart the service and any dependent services.

Note
In Exchange Server 2003, the Exchange Event Service stops automatically if it does not have any work to do. If you are using the ServicesDown Knowledge Script to monitor this service, you get an event every time this service shuts down. If this script is set to restart it, you may get an event every time the script runs if the service continues to stop itself.

Resource Object

Exchange 2000 Server or Exchange Server 2003, Exchange Services folder.

Default Schedule

The default interval is **Every 5 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Automatically re-start service?	Set to **y** to automatically restart down services. The default is y.
Severity: Failed to restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and AppManager could not restart the service. The default is 5 (red event indicator).
Severity: Successful restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and AppManager restarted the service. The default is 25 (blue event indicator).
Severity: Do not restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and you do not want to restart the service. The default is 18 (yellow event indicator).
Check MSExchangeCCMC?	Set to **y** to check the Exchange Connector for Lotus cc:Mail. The default is n.
Check MSExchangeChat?	Set to **y** to check the Microsoft Exchange Chat service. The default is n.
Check MSExchangeCOCO?	Set to **y** to check the Exchange Connectivity Controller. The default is n.
Check MSExchangeDX?	Set to **y** to check the Exchange Directory Synchronization service. The default is y.
Check MSExchangeES?	Set to **y** to check the Exchange Event Service. The default is n.
Check MSExchangeFB?	Set to **y** to check the Exchange Schedule and Free/Busy Connector service. The default is n.
Check MSExchangeGWRtr?	Set to **y** to check the Microsoft Exchange Router for Novell GroupWise. The default is n.
Check MSExchangeIS?	Set to **y** to check the Exchange Information Store service. The default is y.

Description	How to Set It
Check MSExchangeKMS?	Set to y to check the Exchange Key Management Server service. The default is n.
Check MSExchangeMSMI?	Set to **y** to check the MS Mail Connector Interchange service. The default is n.
Check MSExchangeMTA?	Set to **y** to check the Exchange Message Transfer Agent service. The default is y.
Check MSExchangePCMTA?	Set to **y** to check the MS Mail Connector (PC) MTA service. The default is n.
Check MSExchangeSA?	Set to **y** to check the Exchange System Attendant. The default is y.
Check MSExchangeWEB?	Set to **y** to check the Exchange Web Component. The default is y.
Check MSExchangeDS?	Set to **y** to check the Exchange Directory service. The default is y.
Check MSExchangeIMC?	Set to **y** to check the Exchange Internet Mail Connector service. The default is n.
Check MSExchangeSRS?	Set to **y** to check the Site Replication Service. The default is y.
List of services (comma separated)	Specify any additional services you want to monitor. Separate the names by commas with no spaces.

SMTPConnectivity

Use this Knowledge Script to verify connectivity between an Exchange Server and one or more Internet domains through an SMTP gateway. The script verifies connectivity by sending a message to a non-existent user account and examining the resulting non-delivery report (NDR).

Note

Receiving no report is interpreted as a connectivity failure. If you do not allow NDRs, for example, for security reasons, try using the SMTPConnectivityExKnowledge Script, which allows you to send a message to an existing account and examine a delivery report (DR).

If you are checking the domain `netiq.com`, this script sends a test message to `a++++@netiq.com`. This is presumed to be a non-existent account. When the message cannot be delivered to the recipient, the Internet Mail Service sends an NDR to the Exchange mailbox associated with the AppManager agent to indicate the failure. This script scans the subject and body of the NDR for strings that indicate the status of the SMTP gateway host:

- If the test message is delivered to the SMTP host, the NDR says that the user does not exist, but indicates that there is connectivity between Exchange and the SMTP gateway.
- If the test message generates an NDR because it fails to reach the SMTP host, indicates that there is no connectivity between Exchange and the SMTP gateway.

Therefore, to configure this script, you need to know the strings that appear in an NDR subject and body when the domain you are checking is available or unavailable.

If a failover occurs when this script job is running, the job restarts on the new node. It is normal for the job on the failed node to generate one or more error messages, depending on what it was doing when the failover occurred.

To use this Knowledge Script effectively, perform the following before running this script:

1. Verify that your Exchange Server uses the Internet Mail Connector or Internet Mail Service to connect to the Internet through an SMTP gateway.
2. Verify how long it takes the gateway to forward NDRs to the mailbox associated with the AppManager agent service account. If the AppManager agent mailbox does not receive NDRs before the next time it runs, it is considered a connectivity failure.
3. As a test, send an e-mail message to an invalid user account on a valid domain, for example, `a++++@netiq.com`, and see how long it takes for the NDR to come back. If the NDR does not come back before this Knowledge Script runs again, it is interpreted as a domain connectivity failure.
4. If the AppManager agent mailbox successfully receives the NDR, check the subject line and message body for the text strings that indicate the status of the SMTP server. The subject and body text in an NDR can vary for each domain, but typically you can determine the status of the host by checking for the following information:
   - Check the subject line for the keyword string indicating that the test message was not delivered. For example, `Undeliverable` indicates that either the host is unavailable, or the user does not exist, but you cannot tell which until you check the body.
   - Check the body of the message for the same indications. A text string such as `Destination server for this recipient could not be found` indicates no connectivity. A string such as `e-mail account does not exist` means that there is connectivity, even though there is no such account.

   If the subject and the body of the NDR do not help you to determine text strings to use for checking the availability of the SMTP host, try sending a test message to another domain.

5. Repeat this test message when the host is down.

Note

This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event for connectivity status. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns a value of 100 if the connection between the Exchange Server and Internet domain is up or a value of 0 if the connection is down during the interval. The detail message includes the name of each Exchange Server and domain connection checked. When there is connectivity, this script also collects the response time in seconds. The default is y.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange Server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange Server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
List of domains	Specify the domain names that you want to check. If specifying more than one, the Subject and Body Keywords are matched to all of them. Use a pipe character (|) to separate multiple strings. For example: `netiq.com|abc.com` The default domain is netiq.com.

Description	How to Set It
Subject keywords when ...	Provide a keyword string found in the subject line of the NDR message that indicates whether the host status is up or down. • **... host is up**. Enter a keyword string that appears in the subject line of the NDR when mail delivery fails but the host is available. The default is `Undeliverable`. • **... host is down**. Enter a keyword string that appears in the subject line of the NDR when mail delivery fails because the host is not available. The default is `Undeliverable`. If specifying a string for more than one Internet domain, the order in which you specify the keyword strings must correspond to the list of Internet domains. Use a pipe character (|) to separate multiple strings. **Note** Depending on your environment, you may need to set keyword strings for both the subject line and the message body to determine the availability of the host server. For more information, see "Understanding How Keyword Strings Work" on page 162. If you do not specify a value for a parameter, the parameter always matches. If you do not want to use a particular parameter to determine connectivity, you can enter a "garbage" string that does not appear in the NDR.
Body keywords when ...	Provide a keyword string found in the body of the NDR message that indicates whether the host status is up or down. • **... host is up**. Enter a keyword string that appears in the message body of the NDR when mail delivery fails but the host is available. The default is `e-mail account does not exist`. • **... host is down**. Enter a keyword string that appears in the message body of the NDR when mail delivery fails because the host is not available. The default is `destination server for this recipient could not be found`. If specifying a string for more than one Internet domain, the order in which you specify the keyword strings must correspond to the list of Internet domains. Use a pipe character (|) to separate multiple strings. **Note** Depending on your environment, you may need to set keyword strings for both the subject line and the message body to determine the availability of the host server. For more information, see "Understanding How Keyword Strings Work" on page 162. If you do not specify a value for a parameter, the parameter always matches. If you do not want to use a particular parameter to determine connectivity, you can enter a "garbage" string that does not appear in the NDR.
Maximum threshold for a response	Specify the maximum number of seconds in which you expect to get a response. If a response takes longer than this number of seconds, this script raises an event. The default is 120 seconds.
Description file on managed client	Set to **y** to use the keyword strings specified in a file on the managed client to describe the host status. If this parameter is set to y, the subject and body keywords are ignored. The default is n. For more information, see "Understanding How Description Files Work" on page 163.

Description	How to Set It

Description file name	Provide the full path to the file on the agent computer that contains the description file. For example:
	`C:\temp\msgsample.txt`
	To use the specified description file, you must set the Description file on managed client parameter to y.
	The default is `C:\temp\aa.txt`.
	You can use the UNC format to specify the path. For example:
	`\\ENG\appdev\mylog.txt`
	Tip You can only specify one file name for any job instance. To monitor multiple files, create separate Knowledge Script jobs.

Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event. The default is 5 (red event indicator).

Understanding How Keyword Strings Work

AppManager compares the text in the subject and message body of the NDR to the Subject and Body keyword strings you specify. As the script runs, it searches the subject and body of the NDR from left to right for a string that matches the string you have specified, including any spaces. The search is not case-sensitive, however, so you can specify the keyword strings in upper, lower, or mixed case.

For NDRs that substitute the SMTP address or host name in the message body, you can simplify the keyword string by using the following:

- `%%` substitutes the SMTP address. For example, if the body of an NDR contains `User a++++@netiq.com does not exist`, you can search for this string by specifying `User %% does not exist`.
- `##` substitutes the host name. For example, if the body of an NDR contains `Host abc.com does not exist`, you can search for this string by specifying `Host ## does not exist`.

If you specify keyword strings for multiple parameters, AppManager uses rules of precedence to determine the status of the host computer. If the script finds a match to the keyword string you specify for either Subject keywords when host is down, Body keywords when host is down, or both, the script reports the host as unavailable, even if there is also a match for the Subject keywords when host is up, Body keywords when host is up, or both. In general, the only time the script reports the host available is if:

- The report subject line contains no matches to the "Subject keywords when host is down" keyword string, and...
- The report body contains no matches to the "Body keywords when host is down" keyword string, and...
- The report contains matches for both the "Subject keywords when host is up" keyword string and "Body keywords when host is up" keyword string.

If you do not specify a text string for a parameter, the parameter is always considered a match. To configure a parameter to never match, enter a "garbage" text string that does not appear anywhere in the NDR.

Using Keyword Strings to Determine Availability

To configure this Knowledge Script, you must provide specific strings that indicate whether a domain host is available for mail delivery. To do this, you must be familiar with the content of delivery reports (DRs) and NDRs and how to select an appropriate string for which to search.

You can configure this script to identify the host status using the following keyword strings:

Parameter	What to Specify
Subject keywords when host is up	Undeliverable
Subject keywords when host is down	Mail System Error - Returned Mail
Body keywords when host is up	The recipient name is not recognized
Body keywords when host is down	Host netiq.com not found

Understanding How Description Files Work

You can configure this Knowledge Script to use keyword strings specified in the Values tab of the Knowledge Script Properties dialog box or a *description file* on the agent computer.

A description file resides on the agent computer and specifies the keyword strings for one or more Internet domains. If you are monitoring more than one Internet domain, you can use a description file instead of entering keyword strings in the Values tab in the Knowledge Script properties.

If you are using SMTPConnectivity, the account `a++++` is automatically added to the domain name for the test.

If you are using SMTPConnectivityEx, you must specify the account name, such as `a++++@abc.com` or `testaccount@def.com`.

The following parameters are used in the description file to determine the host status. You can specify these parameters at the beginning of the file (followed by a list of domain accounts) or after a single domain name:

- **UpSubject**. Type a keyword string that appears in the report subject line when the host is available.
- **DownSubject**. Type a keyword string that appears in the report subject line when the host is not available.
- **UpBody**. Type a keyword string that appears in the body of the report when the host is available.
- **DownBody**. Enter a keyword string that appears in the body of the report when the host is not available.

Note
If you do not specify a parameter, the parameter definition from the previous domain is used, if one was specified.

Here is a sample description file for **SMTPConnectivity** that uses the same Subject and Body keywords to check the `NetIQ Corporation` and `ABC` Internet domains:

```
UpSubject = “undelivered report”
DownSubject = “undelivered report”
UpBody = “user not found”
DownBody = “host not found”
[netiq.com]
[abc.com]
```

Here is a sample description file for SMTPConnectivityEx that describes three Internet domains. Note the use of the account names when using this script. The first domain (`netiq.com`) uses different keywords than the second domain (`abc.com`). The third domain (`def.com`) reuses the Subject and Body keywords from the second domain:

```
[a++++@netiq.com]
UpSubject = “undelivered report”
DownSubject = “undelivered report”
UpBody = “user not found”
DownBody = “host not found”

[testaccount@abc.com]
UpSubject = “delivery complete”
DownSubject = “non-delivered report”
UpBody = “delivery complete”
DownBody = “host unavailable”

[testaccouunt@def.com]
```

Checking Connectivity for Multiple Domains

To monitor more than one Internet domain and specify the host status parameters in the Values tab of the Knowledge Script properties dialog box, use only the specified keyword strings for each domain. The order in which you specify the keyword strings must correspond to the order in which you list the Internet domains, and you must use the pipe character (|) to separate the strings.

To monitor more than one Internet domain and specify the host status parameters in a description file rather than as a text string for each parameter, use the parameter definition for the previous domain. For more information, see “Understanding How Description Files Work” on page 163.

SMTPConnectivityEx

Use this Knowledge Script to verify connectivity between an Exchange Server and one or more accounts at various Internet domains through an SMTP gateway. It does this by sending a message to a user account (either real or non-existent) and examining the resulting delivery report (DR) or non-delivery report (NDR).

This script scans the subject and body of the report for specific strings that indicate the status of the SMTP gateway host:

- If the test message is sent successfully to the SMTP host, and the message generates either a DR or an NDR, it indicates that the SMTP host is available and there is connectivity between Exchange and the SMTP gateway.
- If the test message generates an NDR because it fails to reach the SMTP host, it indicates that there is no connectivity between Exchange and the SMTP gateway.

Therefore, to configure this script, you need to know the strings that appear in the DR and NDR subject and body that indicate the delivery status.

If no report is received, it is interpreted as a connectivity failure.

If a failover occurs when this script job is running, the job restarts on the new node. It is normal for the job on the failed node to generate one or more error messages, depending on what it was doing when the failover occurred.

To use this Knowledge Script effectively, do the following before running this script:

1. Verify that your Exchange Server uses the Internet Mail Connector or Internet Mail Service to connect to the Internet through an SMTP gateway.
2. Verify the gateway forwards DRs to the mailbox associated with the AppManager agent service account as soon as they are received. If the AppManager agent mailbox does not receive DRs immediately, AppManager cannot accurately report the status of the SMTP host or the connectivity between the Exchange Server and the SMTP gateway.
3. If you do not allow NDRs, set up a user account for this script to use and ensure it sends a DR for successful deliveries.
4. As a test, send an e-mail message to both valid and invalid accounts on a valid domain and see how long it takes for the report to come back. If the report does not come back before the next time the script runs, it is interpreted as a connectivity failure.
5. If the AppManager agent mailbox successfully receives the DR, check the subject line and message body for the text strings that indicate the status of the SMTP server. The subject and body text in a DR can vary for each domain, but typically you can determine the status of the host by checking for the following information:
   - Check the subject line for a keyword string that indicates whether the test message was delivered. For example, `Delivered` means that the host is available, and the user exists. `Undeliverable` means either the host is unavailable, or the user does not exist, but you cannot tell which until you check the body. For each domain, identify the keywords that indicate the status of the server in the subject line.
   - Check the body of the message for a keyword string that indicates whether the test message was delivered. For example `Was delivered`. A text string such as `Destination server for this recipient could not be found` indicates no connectivity. A string such as `e-mail account does not exist` means that there is connectivity, even though there is no such account.

If the subject and the body of the DR do not help you to determine text strings to use for checking the availability of the SMTP host, try sending a test message to another domain.

6. To generate an NDR that indicates the host is down, send the test message when the domain is not available.

Note

This script requires the Exchange MO services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 15 minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event for connectivity status. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns a value of 100 if the connection between the Exchange Server and Internet domain is up or a value of 0 if the connection is down during the interval. The detail message includes the name of each Exchange Server and domain connection checked. When there is connectivity, this Knowledge Script also collects the response time in seconds. The default is y.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange Server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange Server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.

Description	How to Set It
Target domain account(s)	Specify the accounts at the domain names that you want to check. If specifying more than one, the order in which you specify the Internet domains must correspond to the list of Subject and Body Keywords. Use a pipe character (|) to separate multiple strings. For example: `a++++@abc.com|b++++@abc.com|a++++@xyz.com` The default domain account is a++++@netiq.com.
Subject keywords when ...	Provide a keyword string found in the subject line of the NDR message that indicates whether the host status is up or down. • **... host is up**. Enter a keyword string that appears in the subject line of the NDR when mail delivery fails but the host is available. The default is `Undeliverable`. • **... host is down**. Enter a keyword string that appears in the subject line of the NDR when mail delivery fails because the host is not available. The default keyword is `Undeliverable`. If specifying a string for more than one Internet domain, the order in which you specify the keyword strings must correspond to the list of Internet domains. Use a pipe character (|) to separate multiple strings. **Note** Depending on your environment, you may need to set keyword strings for both the subject line and the message body to determine the availability of the host server. For more information, see "Understanding How Keyword Strings Work" on page 162. If you do not specify a value for a parameter, the parameter always matches. If you do not want to use a particular parameter to determine connectivity, you can enter a "garbage" string that does not appear in the NDR.
Body keywords when ...	Provide a keyword string found in the body of the NDR message that indicates whether the host status is up or down. • **... host is up**. Enter a keyword string that appears in the message body of the NDR when mail delivery fails but the host is available. The default message is `e-mail account does not exist`. • **... host is down**. Enter a keyword string that appears in the message body of the NDR when mail delivery fails because the host is not available. The default message is `destination server for this recipient could not be found`. If specifying a string for more than one Internet domain, the order in which you specify the keyword strings must correspond to the list of Internet domains. Use a pipe character (|) to separate multiple strings. **Note** Depending on your environment, you may need to set keyword strings for both the subject line and the message body to determine the availability of the host server. For more information, see "Understanding How Keyword Strings Work" on page 162. If you do not specify a value for a parameter, the parameter always matches. If you do not want to use a particular parameter to determine connectivity, you can enter a "garbage" string that does not appear in the NDR.
Maximum threshold for a response	Specify the maximum number of seconds in which you expect to get a response. If a response takes longer than this number of seconds, this script raises an event. The default is 120 seconds.

Description	How to Set It
Description file on managed client	Set to **y** to use the keyword strings specified in a file on the managed client to describe the host status. If this parameter is set to y, the subject and body keywords are ignored. The default is n. For more information, see "Understanding How Description Files Work" on page 163.

Description file name	Provide the full path to the file on the agent computer that contains the description file. For example:
	`C:\temp\msgsample.txt`
	To use the specified description file, you must set the Description file on managed client parameter to y.
	The default file name is `C:\temp\aa.txt`.
	You can use the UNC format to specify the path. For example:
	`\\ENG\appdev\mylog.txt`
	Tip You can only specify one file name for any job instance. To monitor multiple files, create separate Knowledge Script jobs.

Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event. The default is 5 (red event indicator).

SRSServiceDown

Use this Knowledge Script to monitor the status of the Site Replication Service (SRS). This script attempts to restart a service that is detected as down.

Resource Object

Microsoft Exchange 2000 or Exchange Server 2003

Default Schedule

The default interval is **Every five minutes**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns 100 if the SRS service is running, 0 if the service is not running. The default is n.
Automatically re-start service?	Set to **y** to automatically restart the SRS service if it is down.
Event severity: Failed to restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SRS service is down and AppManager cannot restart the service. The default is 5 (red event indicator).
Event severity: Successful restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SRS service is down and AppManager restarted the service. The default is 25 (blue event indicator).
Event severity: Do not restart	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the SRS service is down and you do not want to restart the service. The default is 18 (yellow event indicator).

TopNISMailboxRes

Use this Knowledge Script to monitor the file space used by the top private information store folders or mailboxes. This script raises an event if the file space for a specified number of mailboxes or folders exceeds the threshold you set.

If a failover occurs while this Knowledge Script job is running, the job restarts on the new node. It is normal for the job on the failed node to generate one or more error messages, depending on what it was doing when the failover occurred.

Note
This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns information about the file space (in MB) used by the top *n* number of folders or mailboxes combined. The default is n.
Monitor the top N mailboxes	Specify the number of top mailboxes you want to monitor. For example, to see the five mailboxes that use the most file space, enter 5. The default is 10. Enter 0 to include all mailboxes.
Maximum threshold for file space size (MB)	Specify the maximum file space size that private information store mailboxes can have before an event is raised. The default is 300 MB.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.

Description	How to Set It
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Character to separate fields in detail message	Provide a character or string of characters to separate each field of data in the event detail message and graph data details. The default character, Null, specifies a Tab character which represents a fixed column width defined within the Knowledge Script.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

TopNISPublicRes

Use this Knowledge Script to monitor the file space used by the top public information store folders (public folders). This script raises an event if the file space for a specified number of public folders exceeds the threshold you set.

Note

This script requires the AppManager agent services to run as a Windows user account with an associated Exchange profile and mailbox. For more information on setting up Exchange mailboxes and profiles, see your Exchange documentation. If you have configured the agent services to run under a Windows user account and provided mailbox and profile information through the setup program or AppManager Security Manager, you can leave the following two parameters blank when you run this script:

- Exchange profile for `NetIQmc` log on as account
- Mailbox alias for `NetIQmc` log on as account

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns information about the total file space used by the top *n* number of folders. The default is n.
Monitor top N folders	Specify the number of top public folders you want to monitor. For example, to see the five folders that use the most file space, enter 5. The default value is 10. Enter 0 to include all public folders.
Maximum threshold for file space size (MB)	Specify the maximum file space size that public information store folders can have before an event is raised. The default is 300 MB.
Exchange profile for NetIQ Corporationmc log on as account	Provide a profile name to use if you do not want to use the default profile names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.
Mailbox alias for NetIQ Corporationmc log on as account	Provide a mailbox alias name to use if you do not want to use the default mail alias names entered in AppManager Security Manager for each Exchange server. **Tip** In most environments, leave this field blank to use the defaults set through AppManager Security Manager.

Description	How to Set It
Character to separate fields in detail message	Provide a character or string of characters to separate each field of data in the event detail message and graph data details. The default character, Null, specifies a Tab character which represents a fixed column width defined within the Knowledge Script.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

TopNReceivers

Use this Knowledge Script to monitor which users received the most mail messages and the total file size of mail messages received by the top users or all users. You can specify the number of top users and the tracking period for when mail messages have been received.

To use this script, you must enable tracking logs. Tracking logs are implemented using the network share `<servername>.log` in Exchange 2000 or Exchange Server 2003 and `tracking.log` in earlier versions. The shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share. If you install Exchange server on a Microsoft cluster, make sure the network share exists on all cluster nodes.

This script reports 0 messages received if you delete the tracking logs or do not enable them.

Note
Daily Exchange server logs begin and end at midnight using Coordinated Universal Time (UTC) rather than local time. This script adjusts for your time zone.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event when a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of mail messages received by the top *n* number of users. The default option is n. **Hint** To collect data to display in the Report_TopNReceivers report, also enable data detail archiving: 1. On the **Advanced** tab, ensure the **Do not archive data detail** option is not selected. 2. Click **OK**.
Detail level (0-2) for event detail message	Specify the level of information that you want to include in the event detail message. The default is 0 which includes the total file size of all messages received by a user. Additional information is available by specifying a detail level: • **0** monitors total file size of messages • **1** monitors the number of messages • **2** monitors file size and number of messages. The default is 2.
Maximum threshold for total file size (MB)	Specify the maximum file size that all messages can have before an event is raised. The default is 300 MB.

Description	How to Set It
Maximum threshold for total number of messages	Specify maximum number of messages that can exist before an event is raised. The default is 1000 messages.
Monitor top N receivers	Specify the number of top users you want to monitor. For example, to see the five users who have received the most e-mail in the period, enter 5. The default value is 3.
Count past N days (including today)	Specify the number of days to use as a tracking period. The default value is 5 (the past 4 days plus today). If you set this value higher than the actual number of daily tracking logs available, the value is reset to the actual number of daily logs. For example, if you set the value to 8 but there are only 5 daily logs available, the value is changed to 5.
Character to separate fields in detail message	Provide a character or string of characters to separate each field of data in the event detail message and graph data details. The default character, Null, specifies a Tab character which represents a fixed column width defined within the Knowledge Script.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

TopNSenders

Use this Knowledge Script to monitor which users sent the most mail messages recently. This script monitors the total file size of mail messages sent by the top users or all users. You can specify the number of top users and the tracking period for when mail messages have been sent.

To use this script, you must enable the tracking logs. Tracking logs are implemented using the network share `<servername>.log` in Exchange 2000 or Exchange Server 2003 and `tracking.log` in earlier versions. The shared directory must exist on the target computer for this script to work properly. By default, the Exchange server installation program sets up the share. If you install Exchange server on a Microsoft cluster, make sure the network share exists on all cluster nodes.

This script reports 0 messages sent if you delete the tracking logs or do not enable them.

Note
Daily Exchange server logs begin and end at midnight using Coordinated Universal Time (UTC) rather than local time. This script adjusts for your time zone.

Resource Object

Exchange 2000 Server or Exchange Server 2003

Default Schedule

The default interval is **Every 24 hours**.

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event?	Set to **y** to raise an event when a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If enabled, data collection returns the number of mail messages sent by the top *n* number of users. The default option is n. **Hint** To collect data to display in the Report_TopNSenders report, also enable data detail archiving: 1. On the **Advanced** tab, ensure the **Do not archive data detail** option is not selected. 2. Click **OK**.
Detail level (0-2) for event detail message	Specify the level of information that you want included in the event detail message. The default specifies the total file size of all messages sent by a user. Additional information is available by specifying a detail level: • **0** monitors total file size of messages • **1** monitors the number of messages • **2** monitors file size and number of messages. The default value is 2.
Maximum threshold for total file size	Specify the maximum size that sent files can attain before an event is raised. The default is 300 MB.

Description	How to Set It
Maximum threshold for total number of messages	Specify the maximum number of messages that can be sent before an event is raised. The default is 1000 messages.
Monitor top N senders	Specify the number of top users you want to monitor. For example, to see the five users who have sent the most e-mail in the period, enter 5. The default value is 3.
Count past N days (including today)	Specify the number of days to use as a tracking period. The default value is 5 (the past 4 days plus today). If you set this value higher than the actual number of daily tracking logs available, the value is reset to the actual number of daily logs. For example, if you set the value to 8 but there are only 5 daily logs available, the value is changed to 5.
Character to separate fields in detail message	Specify a character or string of characters to separate each field of data in the event detail message and graph data details. The default character, Null, specifies a Tab character which represents a fixed column width defined within the Knowledge Script.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 5 (red event indicator).

Appendix A
Performing a Silent Installation

This chapter explains how to install AppManager for Microsoft Exchange 2000 or 2003 silently over a network using a silent installation file that specifies the profiles used during the installation.

Understanding Silent Installation

Performing a silent installation allows you to install AppManager for Microsoft Exchange 2000 or 2003 without any user intervention. Before you run the setup in a silent mode, create the `Exchange-configWizard_out.xml` file that records all the profiles used during installation.

Once you create the `Exchange-ConfigWizard_out.xml` file, run the setup program using a special command line option to read the variables in the `Exchange-ConfigWizard_out.xml` file and install the module accordingly.

Creating the Exchange Installation File

The silent installation file `Exchange-ConfigWizard_out.xml`, contains the profile variables and values that you can use while installing the module. You can create the silent installation file in one of the following ways:

To create the installation file using ckExch2K.exe

1. Copy `ckExch2K.exe` to the `AppManager\bin` folder on the computer where you installed the AppManager 7.0.1 agent.

   Note
   Ensure that you have Exchange server running on this computer.

2. Create `Exchange-ConfigWizard.xml` in the `AppManager\bin` folder with the following content:

```
<?xml version="1.0" standalone="yes"?>
<!DOCTYPE ConfigWizard SYSTEM "ConfigWizard.dtd" [
<!-- Begin Document Specific Declarations -->
<!-- End Document Specific Declarations -->
]>
<ConfigWizard Title="AppManager for Microsoft Exchange Server 2000/2003
Configuration">
<Parameter>
</Parameter>
<WizScript>
      <Page Index="1" UnitCol="0">
<Title>Microsoft Exchange Server Information</Title>
```

```
<Description>Please enter the specified information for monitoring the instances
of Exchange Server listed.
</Description>
         <Action Function="ImportParameters"
         Para="ckExch2K.exe -confWizSetup"/>
      </Page>
      <Wizard>
        <Action Function="Page" Para="1"/>
      </Wizard>
</WizScript>
</ConfigWizard>
```

3. Run the following command from the `AppManager\bin` folder: `NQConfigWizard.exe Exchange-ConfigWizard.xml` and enter the configuration wizard information.

   The `NQConfigWizard.exe Exchange-ConfigWizard.xml` command creates an `Exchange-ConfigWizard_out.xml` file in the same folder.

To create the installation file manually:

1. Create the `Exchange-ConfigWizard.xml` file manually.
2. Configure the following fields in the `XML` file if you are on a single Exchange server:

Parameter	Description
P_SERVER0	Specify the name of the Microsoft Exchange server you want to configure.
P_MBNAME0	Specify the name of the mail box applicable for the Microsoft Exchange server.
P_PROFILE_NAME0	Specify the profile name applicable for the Microsoft Exchange server.
P_DOMAIN0	Specify the domain where you installed the Microsoft Exchange server.
P_USER0	Specify the username applicable for connecting to an instance of the Microsoft Exchange server.
P_PWDE0	Specify the password applicable for the username.
P_SERVER0	Specify the name of the Microsoft Exchange server you want to configure.

Note
If you are using a clustered environment, specify the above configuration details for each server in the cluster.

Example for a non-cluster Exchange server

```
<?xml version="1.0"  standalone="yes"?><!DOCTYPE ConfigWizard SYSTEM
"ConfigWizard.dtd" [
<!-- Begin Document Specific Declarations -->
<!-- End Document Specific Declarations -->
]>
  <ConfigWizard Title="AppManager for Microsoft Exchange Server 2000/2003
Configuration">
    <Parameter>
      <Param Name="Microsoft Exchange Server Information">
        <Desc>Please enter the specified information for
        monitoring the instances of Exchange Server listed.</Desc>
        <Type>string</Type>
        <Size>128</Size>
        <Delim></Delim>
        <Min>2147483648.000</Min>
        <Max>2147483647.000</Max>
        <ReqInput>0</ReqInput>
        <Value></Value>
        <Folder>1</Folder>
      </Param>
```

```
<Param Name="P_SERVER0" Caption="Information for
Exchange Server Monitoring">
  <Desc>Enter the Exchange username and password to use for
  connecting to an Exchange Server instance.</Desc>
  <Type>string</Type>
  <Size>200</Size>
  <Delim></Delim>
  <Min>2147483648.000</Min>
  <Max>2147483647.000</Max>
  <Range></Range>
  <ReqInput>0</ReqInput>
  <Value>EXCH-DOMSINGLE</Value>
  <Parent>Microsoft Exchange Server Information </Parent>
  <Folder>2</Folder>
</Param>
<Param Name="P_MBNAME0" Caption="Mailbox Name">
  <Desc>Enter a mailbox name to be used to send test
  mail from server to server.</Desc>
  <Type>string</Type>
  <Size>300</Size>
  <Delim></Delim>
  <Min>2147483648.000</Min>
  <Max>2147483647.000</Max>
  <Range></Range>
  <ReqInput>1</ReqInput>
  <Value>Administrator</Value>
  <Parent>P_SERVER0</Parent>
  <Folder>0</Folder>
</Param>
<Param Name="P_PROFILE_NAME0" Caption="Profile Name">
  <Desc>Enter a profile name that will be used to
  send test mail.</Desc>
  <Type>string</Type>
  <Size>300</Size>
  <Delim></Delim>
  <Min>2147483648.000</Min>
  <Max>2147483647.000</Max>
  <Range></Range>
  <ReqInput>1</ReqInput>
  <Value>Administrator</Value>
  <Parent>P_SERVER0</Parent>
  <Folder>0</Folder>
</Param>
<Param Name="P_DOMAIN0" Caption="Domain">
  <Desc>Enter a domain for the user with access to
  all Exchange Server instances on the host.</Desc>
  <Type>string</Type>
  <Size>300</Size>
  <Delim></Delim>
  <Min>2147483648.000</Min>
  <Max>2147483647.000</Max>
  <Range></Range>
  <ReqInput>1</ReqInput>
  <Value>EXCH-DOMSINGLE2003.local</Value>
  <Parent>P_SERVER0</Parent>
  <Folder>0</Folder>
</Param>
<Param Name="P_USER0" Caption="Username">
  <Desc>Enter a username with access to all Exchange
  Server instances on the host.</Desc>
  <Type>string</Type>
  <Size>300</Size>
  <Delim></Delim>
  <Min>2147483648.000</Min>
  <Max>2147483647.000</Max>
  <Range></Range>
  <ReqInput>1</ReqInput>
  <Value>Administrator</Value>
  <Parent>P_SERVER0</Parent>
  <Folder>0</Folder>
</Param>
<Param Name="P_PWDE0" Caption="Password">
  <Desc>Enter the password associated with the
  Exchange username specified above.</Desc>
```

```
          <Type>string</Type>
          <Size>300</Size>
          <Delim></Delim>
          <Min>2147483648.000</Min>
          <Max>2147483647.000</Max>
          <Range></Range>
          <ReqInput>1</ReqInput>
          <Value>xxxxxxx</Value>
          <Parent>P_SERVER0</Parent>
          <Folder>0</Folder>
          <I_Type>I_EDIT(2)</I_Type>
        </Param>
      </Parameter>
      <WizScript>
        <Page Index="1" UnitCol="0">
          <Title>Microsoft Exchange Server Information
          </Title>
          <Description>Please enter the specified information for
          monitoring the instances of Exchange Server listed.
          </Description>
          <Item Items="P_SERVER0,P_MBNAME0,P_PROFILE_NAME0,
          P_DOMAIN0,P_USER0,P_PWDE0"/>
        </Page>
        <Wizard>
          <Action Function="Page" Para="1"/>
        </Wizard>
      </WizScript>
    </ConfigWizard>
```

Example for a clustered environment

If you have a two-node cluster with two EVS, the `XML` file contains the following code:

```
<ConfigWizard Title="AppManager for Microsoft Exchange Server 2000/2003
Configuration">
    <Parameter>
      <Param Name="Microsoft Exchange Server Information">
        …
      </Param>
      <Param Name="P_SERVER0" Caption="Information for
      Exchange Server Monitoring">
        …
        <Value>EVS1</Value>
        …
      <Param Name="P_MBNAME0" Caption="Mailbox Name">
…
      <Param Name="P_PROFILE_NAME0" Caption="Profile
      Name">
        …
      <Param Name="P_DOMAIN0" Caption="Domain">
        …
      <Param Name="P_USER0" Caption="Username">
       …
      <Param Name="P_PWDE0" Caption="Password">
      …
      </Param>
      <Param Name="P_SERVER1" Caption="Information for
      Exchange Server Monitoring">
        …
        <Value>EVS2</Value>
        …
      <Param Name="P_MBNAME1" Caption="Mailbox Name">
…
      <Param Name="P_PROFILE_NAME1" Caption="Profile
      Name">
        …
      <Param Name="P_DOMAIN1" Caption="Domain">
        …
      <Param Name="P_USER1" Caption="Username">
       …
      <Param Name="P_PWDE1" Caption="Password">
      …
      </Param>
```

```
 </Parameter>
    <WizScript>
      <Page Index="1" UnitCol="0">
        <Title>Microsoft Exchange Server Information
        </Title>
        <Description>Please enter the specified information
       for monitoring the instances of Exchange Server
       listed.</Description>
<Item items="P_SERVER0,P_MBNAME0,P_PROFILE_NAME0,P_DOMAIN0,P_USER0, P_PWDE0,
P_SERVER1,P_MBNAME1,P_PROFILE_NAME1,P_DOMAIN1,P_USER1, P_PWDE1"/>
      </Page>
      <Wizard>
        <Action Function="Page" Para="1"/>
      </Wizard>
    </WizScript>
  </ConfigWizard>
```

3. Run the following command from the `AppManager\bin` folder: `NQConfigWizard.exe Exchange-ConfigWizard.xml` and enter the configuration wizard information.

   The `NQConfigWizard.exe Exchange-ConfigWizard.xml` command creates an `Exchange-ConfigWizard_out.xml` file in the same folder.

Copying the Installation File to a Directory

After you create the Exchange silent installation file, `Exchange-ConfigWizard_out.xml`, copy the file to a directory where the Exchange AppManager setup program can access the file. For example, copy the file to a folder you have named `c:\ExchSilent`.

Note
If you create the Exchange installation file using `ckExch2K.exe`, also copy the Exchange-ConfigWizard.xml file to the same folder where you copied the Exchange-ConfigWizard_out.xml file.

Running the Setup Program With the Installation File

To install the module silently either from the command line or using a batch script, run the setup program using the following command:

```
msiexec /i  AM70-Exchange2000-7.1.xxx.0.msi /qn MO_CONFIGOUTINI=<full path to the
Exchange-ConfigWizard_out.xml file>
```