Installation and Configuration Guide

Microsoft® Operations Manager 2000 Application Management Pack

Microsoft Corporation

Contents

CHAPTER 1 About the Application Management Pack 1

Introduction 1

What is a Management Pack Module? 1

CHAPTER 2 Installing The Application Management Pack 3

Installation 3

Permissions Required for Installation 3

Application Pack Disk Space Requirements 4

Express Installation: All Components on One Computer 5

Typical and Custom Installations: Installing Components on Multiple Computers 5

CHAPTER 3 Management Pack Module Features and Configurations 9

Microsoft Exchange 2000 Management Pack Module 9

Microsoft Exchange 5.5 Management Pack Module 23

Microsoft Proxy Server Management Pack Module 29

Microsoft ISA Server Management Pack Module 30

Microsoft Site Server 3.0 Management Pack Module 31

Microsoft SNA Server 4.0 Management Pack Module 32

Microsoft Host Integration Server 2000 Management Pack Module 33

Microsoft SQL Server™ Management Pack Module 35

Microsoft Application Center 2000 Management Pack Module 37

CHAPTER 1

About the Application Management Pack

Introduction

The Microsoft® Operations Manager 2000 (MOM) Application Management Pack is a set of Management Pack modules and reports that facilitate the monitoring and management of Microsoft Server products, and improve the availability, performance, and security of Microsoft networks and server applications. With the Application Management Pack, MOM provides central monitoring and automatic problem resolution for networks of tens to thousands of computers, continuously monitoring application software, and servers.

What is a Management Pack Module?

Microsoft Corporation provides many predefined, out-of-the-box solutions called *Management Pack modules*. Management Pack modules are ready-to-use knowledge for monitoring and managing specific applications and environments, such as Exchange or Microsoft SQL Server™ 2000.

Management Pack modules provide predefined computer groups and processing rules, such as filters, alerts, and performance sampling and threshold rules. Management Pack modules also provide predefined computer attributes, providers, scripts, links to the Microsoft Knowledge Base, public views, and default notification groups. These elements integrate specialized research and expertise into your enterprise network. You can load Management Pack modules during setup.

The following Management Pack modules are included in Application Management Pack version 1.0:

- Microsoft Exchange versions 5.5 and 2000
- Microsoft Proxy Server
- Microsoft Internet Security and Acceleration Server 2000
- Microsoft Site Server
- Microsoft Commerce Server 2000
- Microsoft SNA Server version 4.0
- Microsoft Host Integration Server 2000
- Microsoft SQL Server versions 7.0 and 2000
- Microsoft Application Center 2000

For details about how to create a Management Pack module, see the MOM Help.

For the latest issues affecting Management Pack modules, read the release notes on the Microsoft Operations Manager 2000 Application Management Pack 1.0 product CD.

CHAPTER 2

Installing The Application Management Pack

Installation

Before installing the Application Management Pack on a MOM configuration based on either a typical or a custom installation, you must first understand your environment and the MOM architecture. For more information on MOM architecture, see the *User Guide* and the *Installation Guide* that shipped with Microsoft Operations Manager 2000.

Before proceeding with the Application Management Pack installation, it is highly recommend that you perform a complete backup of the OnePoint database on each MOM database computer prior to installing the Application Management Pack. If you are installing MOM SP1, be aware that you must install the Application Management Pack on the DCAM, MOM database, and any MOM Reporting servers.

You should also read the release notes from the MOM product CD, and those from the Application Management Pack, before attempting installation.

Permissions Required for Installation

Before you attempt to install the Application Management Pack, make sure you have the permissions required based on your MOM installation type.

If your installation of MOM is an Express installation, you must be a member of either the Users or the Administrators local group to install this Management Pack.

If your installation of MOM is a Typical or Custom installation with all components on one computer, you must be a member of one of the following local groups in order to install this Management Pack:

- OnePointOp ConfgAdmns
- OnePointOp Operators
- OnePointOp System

If your installation of MOM is a Typical or Custom installation with components installed on multiple computers, you must be a member of the Administrators local group to install this Management Pack.

Application Pack Disk Space Requirements

Database:

If all the Management Pack modules are installed, 65 megabytes (MB) of available space in the OnePoint database is used. If only some of the Management Pack modules are selected for installation, space requirement will be changed to reflect that.

MOM Reporting Folder:

A backup of the existing database file is created and the new database file is copied to the MOM Reporting folder, using about 25 MB of disk space on the drive where that folder is located.

Temp folder:

During the Application Management Pack installation, the setup files are expanded into the user's Temp folder. The drive where the Temp folder is located must have at least 70 MB of space free for installation.

Express Installation: All Components on One Computer

▻ **To install the Application Management Pack on an Express setup MOM configuration where the database and central MOM components are on a single computer:**

1. Log on to the central computer with a Microsoft Windows® 2000 administrator account.
2. Close all open applications.
3. Back up the MOM database.
4. Insert the product CD in the drive.
5. Read the Release Notes.
6. Click the AppPack Setup link on the Setup screen and follow the on-screen instructions.

> **Note**
>
> During installation, you will see the **Import Selection** dialog box. You will need to choose which import option you want for your installation. If you are upgrading an existing Management Pack module, improper selection can result in loss of modified rules, custom rules, or company knowledge. See "Choosing An Appropriate Import Selection Option" later in this chapter for more information.

Typical and Custom Installations: Installing Components on Multiple Computers

> **Note**
>
> In a custom configuration, the Application Management Pack must be installed on each MOM database, central, and reporting computer. No installation is necessary on MOM Administrator console or agent computers.

Installation on MOM Database Computers

When installing the Application Management Pack on a Typical or Custom setup MOM configuration where the Database, Central, and/or Reporting MOM components are on one or more computers, Setup will automatically limit the available installation components to those that are applicable to the target computer. In the case of the database computer, only the Application Management Pack database views will be available for installation.

As a best practice for installing the Application Management Pack in a custom configuration, install the product first on the database computer, then on the central computer and, finally, on all reporting computers.

To install:

1. Log on to the MOM computer with a Windows 2000 administrator account.
2. Close all open applications.
3. Backup the database on the MOM database computer.
4. Insert the product CD.
5. Read the Release Notes (RelNotes.htm).
6. Click the AppPack Setup link on the Setup screen and follow the on-screen instructions.

Installation on MOM Central Computers

When installing the Application Management Pack on one or more central computers, Setup will automatically limit the available installation components to those that are applicable to the target computer. In the case of the central computer, only the Application Management Pack Management Pack modules will be available for installation.

To install:

1. Log on to the MOM computer with a Windows 2000 administrator account.
2. Close all open applications
3. Insert the product CD in the drive.
4. Read the Release Notes.
5. Click the AppPack Setup link on the Setup screen and follow the on-screen instructions.

Note

During installation, you will see the Import Selection dialog box. You will need to choose which import option you want for your installation. If you are upgrading an existing Management Pack module, improper selection can result in loss of modified rules, custom rules, or company knowledge. See “Choosing An Appropriate Import Selection Option” later in this chapter for more information.

Installation on MOM Reporting Computers

When installing the Application Management Pack on one or more reporting computers, setup will automatically detect and limit the available installation components to those that are applicable to the target computer. In the case of the reporting computer, only the Application Management Pack **Reporting** will be available for installation.

To install:

1. Log on to the MOM computer with a Windows 2000 administrator account.
2. Close all open applications
3. Insert the product CD into the drive.
4. Read the Release Notes.
5. Click the AppPack Setup link on the Setup screen and follow the on-screen instructions.

Choosing an Appropriate Import Selection Option

During installation, you will see the **Import Selection** dialog box. You will need to choose which import option you want for your installation. Review each option listed below before proceeding with the Application Management Pack installation.

Merge Existing Management Pack

This option merges an existing Management Pack module with the new version that is being imported. The merge results in the following:

- User-added company knowledge on vendor-shipping rules is retained.
- All user-added custom rules are retained.
- User-modified rules, scripts, data providers, and computer groups on vendor-shipping rules are overwritten.

This option is recommended if you want to completely synchronize the existing Management Pack with the latest version and retain company knowledge and custom rules.

Replace Existing Management Pack

This option replaces an existing Management Pack module with the new version that is being imported. The replace results in the following:

- User-added company knowledge on vendor-shipping rules is removed.
- All user-added custom rules are removed.
- User-modified rules, scripts, data providers, and computer groups on vendor-shipping rules are overwritten.

This option is the recommended if you want a fresh installation of the latest Management Pack, and you do not want to retain any user-created company knowledge or custom rules.

Post Installation Procedures

After you have successfully installed the Application Management Pack on your MOM configuration, the Management Pack module rules will not instantly be deployed. Instead, rules will be deployed to the managed computers at the next scheduled scan or the next heartbeat, whichever comes first. If you wish to expedite the deployment of the Application Management Pack rules to your managed computer, you can perform a managed computer scan manually.

▻ To scan managed computers:

1. Expand **Microsoft Operations Manager** in the left pane.
2. Expand **Configuration** in the left pane.
3. Click **Global Settings** in the left pane.
4. Click **Agent Managers** in the right pane.
5. Click **Action** on the menu bar and select **Properties**.
6. If you want to change the time and frequency that agent managers automatically scan managed computers, specify the desired values on the **Managed Computer Scan** tab.
7. If you want the agent manager to perform a scan now, click **Scan managed computers now** on the **Managed Computer Scan** tab.
8. Click **Pending Installations** in the left pane to see the results of the scan.

CHAPTER 3

Management Pack Module Features and Configurations

Microsoft Exchange 2000 Management Pack Module

The following sections describe the purpose, features, configuration, and default notification group of the Microsoft Exchange 2000 Management Pack module for MOM.

Purpose

The Microsoft Exchange 2000 Management Pack module monitors the performance, availability, and security of Microsoft Exchange 2000 Server. In addition to Microsoft Exchange Server, this Management Pack module provides a complete Microsoft Exchange solution by monitoring access to Active Directory, information store, extensible storage engine, message transport, Exchange clustering, Outlook Web access, and Internet protocols (such as SMTP, POP, and IMAP). By detecting, alerting on, and automatically responding to critical events, this Management Pack module helps indicate, correct, and prevent possible Exchange service outages.

This Management Pack module monitors many significant Exchange performance counters. Using performance thresholds and related alert definitions to highlight performance conditions that may indicate service problems or possible denial of service attacks, this Management Pack module allows you to identify issues before they become critical. Increasing the security, availability, and performance of your Microsoft Exchange installation, this Management Pack module reduces your cost of ownership by enabling proactive Exchange management.

The Exchange 2000 Management Pack also contains an array of scripts to monitor single, and cross-server usage, performance, reliability, and configuration. This Management Pack monitors all configurations of Exchange 2000 servers, including standalone servers and clusters, as well as front-end and back-end servers.

Features

The Microsoft Exchange Management Pack module monitors events that are placed in the Application event log by various components of Exchange, such as directory service access, information store, extensible storage engine, message transfer agent, Exchange clustering, Outlook Web access, and Internet protocols.

This Management Pack module includes key performance metrics to monitor the overall performance of Microsoft Exchange, and to alert you to critical performance issues. Using MOM Reporting, you can analyze and graph this performance data to understand usage trends, to perform accurate load balancing, and to manage system capacity.

With extensive embedded expertise, this Management Pack module allows you to proactively manage your Exchange installation and avoid costly service outages. For example, this Management Pack module performs the following tasks to alert you of possible critical conditions:

- Monitors vital performance monitor data, which can indicate that the server is running low on resources.
- Collects important warning and error events from Exchange 2000 servers, and alerts operators to problems.
- Monitors disk capacity and alerts operators when disk capacity is running low. Provides knowledge about which Exchange files are on the affected drives.
- Monitors the Exchange services that are expected to be running on a specific server.
- Monitors whether an Exchange database can actually be reached by a MAPI client logon. This verifies both the Exchange database and the Active Directory functionality.
- Monitors high queue lengths that are caused by an inability to send e-mail to a destination server.
- Monitors and alerts operation to a high number of simultaneous connections, indicating a denial of service attack
- Monitors configuration errors or resource shortages affecting service levels.

This Management Pack module features saved public views that are Exchange-specific. These views provide a quick snapshot of the health of your Exchange implementation. This Management Pack module also includes many Exchange-specific reports to help you quickly identify and correct Exchange issues.

This Management Pack module quickly brings any service outages or configuration problems to your attention, increasing the security, availability, and performance of your Microsoft Exchange installation.

Reports

Exchange 2000 reports include the following categories of information:

- Exchange 2000 Health Monitoring and Operations reports summarize Exchange 2000 health and usage, server availability, and configuration of Exchange 2000 servers, databases and mailboxes.
- Exchange 2000 Database Size report lists database sizes for Exchange 2000 servers. Database size (in MB) is presented for each server, storage group, and database.
- Exchange 2000 Disk Usage report provides the disk usage of Exchange 2000 servers based on disk performance counters. Daily averages for each counter are presented. Highest average in a 30-minute period for each of the counters is also included, in addition to the time of occurrence of the highest average.
- Exchange 2000 Mailboxes per Server report lists distribution of mailboxes across storage groups and databases for Exchange 2000 servers. The number of mailboxes and maximum limit for mailboxes is presented for each server, storage group, and database.
- Exchange 2000 Server Availability report summarizes the percentage server availability for Exchange 2000 servers during the specified time period. The percentage of availability and unavailability are listed along with the reasons for unavailability.
- Exchange 2000 Server Configuration report provides Exchange 2000 Server configuration information including computer and operating systems configuration, local disks information, Exchange 2000 server and storage group configuration.
- Exchange 2000 Usage and Health report provides Exchange 2000 server usage and health, based on key Exchange and SMTP performance counters. The report presents daily totals and averages for the specified time period. The highest average for each counter in a 30-minute period is also included with the time of occurrence for the highest average.
- Exchange Capacity Planning reports summarize the Exchange server resource usage and help you plan for current and future capacity needs.
- Exchange Mailbox and Folder Sizes reports summarize the size of Exchange mailboxes and folders.
- Exchange Performance Analysis reports summarize Exchange performance counters and help you analyze your queue performance.
- Exchange Traffic Analysis reports summarize Exchange mail traffic patterns by message count and size.

▻ To obtain descriptions of all reports in these categories

1. From the **Start** menu, point to **Programs**, point to **Microsoft Operations Manager**, and then click **MOM Reporting**.
2. In the left pane, right-click the report you want, and select **Report Help**.

You can also refer to Help topics under the topic **Report Descriptions**, subtopic **Exchange Server**.

Note

Exchange 2000 Health Monitoring and Operations reports are for Exchange 2000 servers only. The other categories of Exchange reports listed above are applicable to both Exchange 2000 and Exchange 5.5 servers.

Configuration

Some configuration is necessary to use certain components of the Exchange Management Pack.

Upgrading from a pre-Service Pack 1 configuration:

If the deployment to be upgraded was not configured to use Exchange 2000 Management Pack functionality in MOM RTM (which required MAPI logons), then see the “Mailbox Access Account Configuration” section later in this chapter.

For MOM SP1, the Exchange 2000 Management Pack performs all functionalities with the OnePoint service (MOM agent) running as Local System instead of a domain account. This section describes the steps that are needed to make this change.

The rules that require this configuration change are those that use an agent mailbox on each Exchange server:

Processing Rule Group: Server Availability — MAPI Logon Check

Rule Name: Check store availability — MAPI logon

Processing Rule Group: Server Availability — Mail Flow Verification

Rule Name: Send mail flow messages

Rule Name: Receive mail flow messages

Processing Rule Group: Server Utilization Logging: Reporting and Views/Report Collection

Rule Name: Report collection — mailbox statistics

Rule Name: Report collection — public folder statistics

If you deployed the original Exchange 2000 Management Pack functionality to allow the Exchange 2000 Management Pack to access the agent mailboxes (which required OnePoint to run under an account with Domain Administrator privileges — the Agent Service account), follow the instructions in this section to convert to the SP1 Exchange 2000 Management Pack configuration to the latest version.

> **Note**
>
> The Agent Service account, which was used in the pre-SP1 Exchange 2000 Management Pack to denote the account under which OnePoint ran, is now used as the Mailbox Access account. The sole function of the Mailbox Access account is to be the single domain account (without any extraordinary privileges) which can access the agent mailboxes.

Changing the OnePoint service to Local System instead of the Agent Service Account:

1. On each Exchange server being monitored, open the **Services** console. From **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Services**.
2. Double-click the **OnePoint** service to open the **Properties** dialog box.
3. Click the **Log on** tab, under **Log on as:**, and select the **Local System** account.

Removing administrative rights from the Agent Service Account:

1. On any Exchange server, open **Active Directory Users and Computers.** Click **Start**, point to **Programs**, point to **Microsoft Exchange**, and then click **Active Directory Users and Computers**.
2. Open the **Properties** dialog box of the agent account.
3. Under the **Member Of** tab, remove any administrative rights to ensure that it is only a member of Domain Users.

> **Note**
>
> If this account is used for something else outside the Exchange 2000 Management Pack that requires domain administrator rights, the account can be left with Domain Administrator rights.

Change MOM's global setting for agent account service back to the default of the Local System:

1. Open the MOM Administrator console.
2. In the left pane, expand **Configurations/Global Setting**, and in the right pane, double-click **Agent Managers** to open its **Properties** dialog box.
3. Click the **Agent Service Account** tab. Under **Service Account**, select the local system account.

4. In the left pane, expand **Configurations/Agent Managers**, and in the right pane, perform the following steps for each Agent Manager to ensure that it is running under the local system:
   - Double-click the agent manager object to open its **Properties** dialog box.
   - Click the **Agent Service Account** tab
   - Ensure that the **Use Global Setting** check box is selected.

Proceed to the "Store Mailbox Access Account Credentials" section, later in this chapter.

Mailbox Access Account Configuration

To use the functionality, which relies on a MAPI logon to Exchange 2000, at least one agent mailbox must be created on each Exchange server being monitored. To access these mailboxes, the Exchange Management Pack must have a single domain user account — the Mailbox Access account — that can access all the agent mailboxes on all the servers. The agent account also needs to be granted the Exchange View-Only Administrator role in order to collect information about the Exchange server for the Mailbox and Public Folder statistics reports.

> **Note**
> The rules that use the Mailbox Access accounts will not function on a server running Exchange, which is also a Domain Controller.

The rules that require this configuration are those that use an agent mailbox on each Exchange server:

Processing Rule Group: Server Availability — MAPI Logon Check

Rule Name: Check store availability — MAPI logon

Processing Rule Group: Server Availability — Mail Flow Verification

Rule Name: Send mail flow messages

Rule Name: Receive mail flow messages

Processing Rule Group: Server Utilization Logging: Reporting and Views/Report Collection

Rule Name: Report collection — mailbox statistics

Rule Name: Report collection — public folder statistics

> **Note**
> This account is used by scripts in the Exchange 2000 Management Pack to access the test mailboxes. None of these scripts require that Outlook be installed on the Exchange server. Installing Outlook on an Exchange server is not recommended. For more information, see Knowledge Base article Q266418.

To create the Mailbox Access account:

1. Start the **Active Directory Users and Computers** snap-in (dsa.msc).
2. Expand the console tree on the left pane and select Users, then select New, and click User
3. Follow the dialog box directions to complete the new user creation. It is not necessary to create an Exchange mailbox for this account. The **Create Mailbox** dialog box appears only if the Active Directory Users and Computers snap-in is running on a computer with the Exchange System Manager installed.
4. This user account is referred as the Mailbox Access account.

To grant the role of Exchange View-Only Administrator to the Mailbox Access account:

1. On an Exchange server, start **Exchange System Manager**
2. In the left pane, right-click the root object (Organization level), select **Delegate control**, and then click **Next**.
3. In the **Users and Groups** pane, click **Cancel,** if the domain user account you just added as your Mailbox Access account is listed as **Exchange Full Administrator**, **Exchange Administrator**, or **Exchange View Only Administrator**. Otherwise, click **Add**.
4. Under either the **Group** or **User** field, browse for your Mailbox Access account.
5. Under **Role**, select **Exchange View Only Administrator**.
6. Click **OK**, click **Next**, and then click **Finish**.

Store Mailbox Access Account Credentials

To inform the Exchange Management Pack about the Mailbox Access account, perform the following steps:

1. After creating the Mailbox Access accounts, wait until all Exchange managed nodes receive the event **Exchange MOM 9986** (approximately 10-15 minutes).
2. On the MOM server, log on with local administrator credentials to all Exchange servers. For example, log on as a Domain Administrator.
3. In a text file, create a list of all the Exchange managed nodes monitored by MOM. For example, use Notepad to create a file called C:\ExServerList.txt. In the file, list the server names and end the list with a period (**.**):

```
ServerA
ServerB
ServerC
.
```

In the case of an Exchange cluster, these should be the names of the physical servers, *not* the Exchange virtual servers.

1. From the command prompt, navigate to \Program Files\Microsoft Operations Manager 2000\OnePoint.
2. Run the Credential Utility as ExchangeMOMSetCredentialUtility.exe –E <filepath>

   Example: ExchangeMOMSetCredentialUtility.exe –E C:\ExServerList.txt

When running the Credential utility, you are prompted for the credentials of the account to access the agent mailboxes. Respond with the credentials for the Mailbox Access account.

Agent Mailbox Account Creation and Configuration

The following rules require the configuration of an agent mailbox on each Exchange server:

Processing Rule Group: Server Availability — MAPI Logon Check

Rule Name: Check store availability — MAPI logon

Processing Rule Group: Server Availability — Mail Flow Verification

Rule Name: Send mail flow messages

Rule Name: Receive mail flow messages

Processing Rule Group: Server Utilization Logging: Reporting and Views/Report Collection

Rule Name: Report collection — mailbox statistics

Rule Name: Report collection — public folder statistics

> **Note**
>
> Do not create agent mailboxes on front-end Exchange servers.

On an Exchange server:

1. On a computer with the Exchange System Manager installed, start the Active Directory Users and Computers snap-in (dsa.msc), and create a user account and mailbox on each Exchange server with the logon name that includes the name of the Exchange server as **<servername>MOM**. If this is an Exchange cluster, then the server name is the name of the Exchange virtual server. For example, if the server name is ExServer1, then the test account should be ExServer1MOM.

   If you have multiple database files on a server, you can add more test accounts with logon name **<servername>MOM#** where # can be any number or word. The first test account must be named **<servername>MOM**. However, one of the mailboxes must be **<servername>MOM**.

2. Select all of the following during account creation:
   User cannot change password
   Password never expires
   Account is disabled
   Ensure that you create a mailbox for this account.

3. On the **View** menu, select **Advanced Features**.
4. Open the property dialog box of the user account, and then click the **Exchange Advanced** tab. If this tab is not present, ensure that the **Advanced Features** option was selected in the previous step.
5. Click **Mailbox Rights**, and then click **Add**.
6. Add the Mailbox Access account, and then click **OK**.
7. In the **Permissions** box, give the Mailbox Access account **Full Mailbox Access**.
8. Go back to the **Name** box, and select **Self**.
9. Check **Associated external account,** and click **OK**.
10. Click the **Security** tab and select the Mailbox Access account. It might be necessary to click **Add** if the Mailbox Access account is not listed, and select it from the list of all accounts.
11. With the Mailbox Access account selected, in the **Permissions** box, under the **Allow** column, select the **Receive As** and **Send As** boxes, and then click **OK**.

Note

The Agent Mailbox cannot be set to be hidden in the Global Address Book (GAL) because it is not possible to log in to an account in that state.

Service Verification Scripts

Processing Rule Group: Server Availability/Verify Exchange Services

Rule Name: Service verification. Check services script

Periodically, the Service Verification Script runs to determine whether a list of services specified in a registry key on the Exchange server is running.

Note

Service Verification can be configured using the Exchange 2000 Management Pack Configuration Utility, which is available for download at http://www.microsoft.com/downloads/.

Specify the Exchange-related services to be monitored in the following registry key on the managed Exchange servers:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange MOM

It is necessary for the user to create this key.

In this key, create the entry **Monitored Services** as a string. Fill this string with a comma-delimited list of the services for which you want to receive notification if the services are not running.

Example setting for this entry:

MSExchangeIS, MSExchangeSA, MSExchangeMTA, SMTPSVC, POP3SVC, IMAP4SVC

In a cluster configuration, it is necessary to add this entry on each cluster node.

Exchange Traffic Analysis Reports

Processing Rule Group: Server Utilization Logging: Reporting and Views/Report Collection Scripts

Rule Name: Report Collection - Message Tracking Log Data

The Exchange 2000 Management Pack module includes a timed event rule that collects information from the Message Tracking logs and analyzes it to assemble the Exchange Traffic Analysis reports, which detail various aspects of the messaging traffic. It analyzes the message-tracking log for the previous day.

To produce this report, you must configure the Management Pack module to enable message tracking for Exchange as follows:

1. Start **Exchange System Manager**.
2. Locate the **Servers** container.

> **Note**
>
> The Servers container can be at the top level if no Administrative Groups are defined or displayed. If Administrative Groups are defined or displayed, the container can be found in the relevant Administrative Group container.

3. Expand the **Servers** container to see the list of servers.
4. Right-click the server on which you intend to enable tracking, and select **Properties**.

5. On the **General** tab, select the **Enable Message Tracking** check box.
6. Ensure that the log file maintenance information suits the requirements for logging. By default, log files older than seven days are deleted.
7. Verify that the log directory exists and has data coming through. The Exchange log directory is named \\server\server.log for Exchange 2000.

Note

In some cases, Exchange 2000 cannot resolve the sender for a piece of mail from the 1031 message tracking log event used to track sent mail, and this is reported as the sender being "Not available" in the "Exchange 2000 Traffic Analysis" reports:

- SMTP Out - Top 100 Senders by Count
- SMTP Out - Top 100 Senders by Size

This occurs when the mail was sent to a distribution list that is configured as "Do not send delivery reports" on the **Exchange Advanced** tab of the **Distribution List Properties** dialog box. In this case, the Active Directory attributes *reportToOriginator* and *reportToOwner* are both false.

If Send delivery reports to group owner is selected for a distribution list, then all mail sent to this distribution list will have the owner of the list appearing as the sender in the message tracking log.

The default for distribution lists is Send delivery reports to message originator. In this case, Exchange 2000 reports the real sender in the message tracking log.

Mail Flow Verification Script

Processing Rule Group: Server Availability/Mail Flow Verification

Rule Name: Send mail flow messages

Rule Name: Receive mail flow messages

These scripts periodically send mail and verify that the mail has been received. You must configure the sending and receiving servers to know where to send mail, and from where to expect mail.

Note

Mail flow verification can be configured using the Exchange 2000 Management Pack Configuration Utility, which is available for download at http://www.microsoft.com/downloads/.

The mail flow verification uses the same **<*servername*>MOM** mailbox accounts created for the **Server Availability Script - MAPI Logon Check**. See this process rule group for more information on these accounts. For each server participating in the mail flow verification (as senders or receivers, or both) follow these configuration steps:

1. Configure the time interval to send/receive mail according to your Exchange 2000 installation (the default is 15 minutes).
    a. In the current processing rule group folder, right-click the event processing rule named **Send mail flow messages,** and click **Properties** in the right-click menu.
    b. Click the **Data Provider** tab.
    c. Select the desired provider with the type *Timed Event*, and synchronize the provider at 0:00. If necessary, create and synchronize a new provider.
    d. Repeat the same process for the event processing rule **Receive mail flow messages**. Select a timed event with the same frequency as the one selected for **Send mail flow messages,** but synchronize at a different time.
2. To configure the number of failed attempts to receive mail before generating an alert (the default is four attempts).
    a. In the current processing rule group folder, right-click the event processing rule named **Receive mail flow messages,** and click **Properties** in the right-click menu.
    b. Click the **Responses** tab.
    c. Select **Exchange 2000 - Mail flow receiver,** and click **Edit**.
    d. In the **Launch Script** dialog box, double-click the parameter and enter the value you want to use.
    e. Click **OK** in all the dialog boxes.
3. Configure the registry to specify the server, which will send and/or receive mail.
    a. In each Exchange 2000 server (or virtual server), create the following registry key: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange MOM\Mail Flow\<*Servername*>**
    b. If this is in a clustered configuration, the server name should be the Exchange Virtual Server. Create this same key (and the values in the next two instructions) on each physical node of the cluster.
    c. Under this key, create a string value named **SendTo** as string and set its data to a comma-delimited list containing the server names to which mail will be sent. If the server is not going to send mail, keep this registry value empty.

d. Under the same key, create a string value named **ExpectedFrom** as string and set its data to the server name from which mail is expected. If the server is not expecting mail from other servers, keep this registry value empty.

> **Note**
>
> Although not necessary, you can secure the <servername>MOM mailboxes so that they can receive mail from the other test mailboxes that are expected to send mail to this particular mailbox. To do this, on a computer with the Exchange System Manager installed, run the Active Directory Users and Computers snap-in (dsa.msc). Select the user in question, right click and select **Properties**. On the Exchange **General** tab, click **Delivery Restrictions**. In the **Message Restrictions** section, click **Only from**, and add the test mailbox accounts that will send mail to this account.
>
> Test mailboxes that are not used in Mail Flow Verification can be configured to not accept any mail by following the same steps and leaving the **Only from** list blank.

Disk capacity planning:

Plan disk capacity by using views of the disk space used. The data for these views comes from the Logical Disk performance monitor counters. Enable these counters on all monitored Exchange servers by typing **diskperf –y** from a command prompt. You must then reboot the server for this change to take effect.

> **Note**
>
> The Exchange 2000 Management Pack's alerts about low disk space use WMI to get disk space rather than performance counters.

Collect Operating System Server Information Script

Processing Rule Group: Server Utilization Logging: Reporting and Views/Report Collection Scripts

Rule Name: Report Collection – Windows 2000 Server Configuration Information

No particular configuration is necessary for this rule. However, with pre-SP3 configurations of Windows 2000, see the Knowledge Base article Q279225 for a WMI patch to download. This should be applied against all Exchange servers. This patch allows the Exchange 2000 – Collect OS Server Information script to run more reliably. This will be included in Windows 2000 Service Pack.

Using Exchange Reports with Exchange 2000 Clusters

Many of the Exchange reports included in the Exchange 2000 Management Pack require that Exchange virtual server names be included in Managed Computer Rules as managed servers. This is because the reports need to recognize the Exchange virtual servers as an Exchange server.

Best Practice Configuration:

- In a clustered configuration, it is advantageous to disable event log replication to prevent duplicate alerts from the physical cluster nodes. For more information about this configuration, see the Microsoft Knowledge Base article Q224969.
- The mailbox and public folder analyses send the results to the corresponding reports as performance counters with an McExchDG object. Over time, hundreds of counters might accumulate. This accumulation can delay getting a view of all performance counters on a server. Views exist for most Exchange 2000 performance counters in the Management Pack, and in general it is good practice to create additional views for other frequently used performance counters rather than get the list of all performance counters for a given server.
- Total CPU measurements might be inaccurate, because full text indexing consumes all available CPU using low priority threads. If you are using full text indexing, you might want to disable the %CPU rule located in
  Microsoft Windows 2000 Operating System\Windows 2000 — All Computers
  \Threshold Performance Counters for Windows 2000.
- The rules in the Default Event Collection for Microsoft Windows NT and 2000 Management Pack collect all events from monitored servers. Ensure that these rules are disabled for normal operations.
- Consider whether you want to use the service availability reports. These can consume a large amount of space in the MOM database. If they are not needed, disable collecting the service availability events by clearing the **Enable Service Checking and Reporting** option on the **Service Availability** tab in the **Global Agent Settings** dialog box.

Default Notification Group

The default notification group for processing rule responses within the Exchange Management Pack module is Mail Administrators. For information about adding operators to this notification group, see the MOM Help.

Microsoft Exchange 5.5 Management Pack Module

The following sections describe the purpose, features, configuration, and default notification group of the Microsoft Exchange 5.5 Management Pack module for Microsoft® Operations Manager 2000 (MOM).

Purpose

The Microsoft Exchange 5.5 Management Pack module monitors the performance, availability, and security of Microsoft Exchange version 5.5. In addition to Microsoft Exchange Server, this Management Pack module provides a complete Microsoft Exchange solution by monitoring the directory service, database, Internet mail connection, information store, message transfer agent, NNTP interface, and POP3 interface. By detecting, alerting on, and automatically responding to critical events, this Management Pack module helps indicate, correct, and prevent possible Exchange service outages.

This Management Pack module monitors many significant Exchange performance counters. Using performance thresholds and related alert definitions to highlight performance conditions that might indicate service problems or possible denial of service attacks, this Management Pack module allows you to identify issues before they become critical. Increasing the security, availability, and performance of your Microsoft Exchange installation, this Management Pack module reduces your cost of ownership by providing proactive Exchange management.

Although most of the functionality of this management pack works on Exchange 5.5 clustered servers, the scripts are not cluster-aware. As a result, some of the data will not be collected for some of the reports. These include the reports in the folders Exchange 5.5 Traffic Analysis and Exchange Mailbox and Folder Sizes. The Exchange 2000 Management Pack is fully cluster-aware.

Features

The Microsoft Exchange 5.5 Management Pack module monitors events placed in the Application event log by various components of Exchange such as the directory service, database, Internet mail connection, information store, message transfer agent, NNTP interface, and POP3 interface.

This Management Pack module includes key performance metrics to monitor the overall performance of Microsoft Exchange and to alert you to critical performance issues. Using MOM Reporting, you can analyze and graph this performance data to understand usage trends, to perform accurate load balancing and to manage system capacity.

This Management Pack module has extensive embedded expertise, so you can proactively manage your Exchange installation and avoid costly service outages. For example, this Management Pack module alerts you to the following critical conditions:

- Slow delivery times indicating a reduction in the current service level
- High queue lengths resulting in an inability to send mail to or receive mail from the Internet
- High number of simultaneous connections indicating a denial of service attack
- Configuration errors or resource shortages affecting service levels
- Replication errors affecting distributed Exchange directories

This Management Pack module features saved public views that are Exchange-specific. These views provide a quick snapshot of the health of your Exchange implementation. This Management Pack module also includes many Exchange specific reports, to help you quickly identify and correct Exchange issues.

This Management Pack module quickly brings any service outages or configuration problems to your attention. This increases the security, availability, and performance of your Microsoft Exchange installation.

Reports

Exchange 5.5 reports include the following categories of information:

- Exchange 5.5 Operations reports graph Exchange 5.5 counters for Internet news and e-mail, replication, delivery times, and queue lengths. These reports are for Exchange 5.5 servers only.
- Exchange Capacity Planning reports summarize the Exchange server resource usage and help you plan for current and future capacity needs.
- Exchange Mailbox and Folder Sizes reports summarize the size of Exchange mailboxes and folders.
- Exchange Performance Analysis reports summarize Exchange performance counters and help you analyze your queue performance.

- Exchange Traffic Analysis reports summarize Exchange mail traffic patterns by message count and size.

For descriptions of all reports in these categories:

1. From the **Start** menu, point to **Programs**, point to **Microsoft Operations Manager**, and then click **MOM Reporting**.
2. In the left pane, right-click the report you want, and select **Report Help**.

You can also refer to Help topics under the topic **Report Descriptions**, subtopic **Exchange Server**.

Exchange 5.5 Operations reports are for Exchange 5.5 servers only. The other categories of Exchange reports listed above are applicable to both Exchange 5.5 and Exchange 2000 servers.

Configuration

The following versions are required for the scripts included in this Management Pack module to work correctly:

- Microsoft Exchange version 5.5 with Service Pack 2 or later
- Microsoft Outlook® 2000

> **Note**
>
> With Outlook 2000, you must load the CDO option. This option is not loaded by default.

To benefit from the Microsoft Exchange Management Pack module and reports, you must configure Exchange to produce at least minimum logging.

To configure Exchange 5.5 to produce logging

1. Log on to the Microsoft Exchange server as an Exchange Administrator.
2. Click **Exchange Administrator** in the Microsoft Exchange program folder.
3. Expand the **Organization** list, the **Site** list, the **Configuration** list, and then the **Servers** list.
4. Select the server you want to monitor with MOM.
5. Click **Properties** on the **File** menu.
6. Click the **Diagnostics Logging** tab.
7. Select a service in the **Services** list box.
8. Select all the categories in the **Category** list box.
9. Click **Minimum**, **Medium**, or **Maximum**, depending on the amount of logging desired.
10. Repeat steps 11 through 13 for all the services, and then click **OK**.
11. Click **Exit** on the **File** menu.

Logging levels include:

- None — Logs only critical and error events.
- Minimum — Logs high-level events by writing one entry for each major task the service performs. This can help identify where a problem is occurring.
- Medium — Records entries for each step taken to run a task. This gives more detail when the problem is located.
- Maximum — Records entries for each line of code in the service, providing a complete trail of the service operation. Logs all events. This creates a large amount of data, which can affect server performance.

Some Exchange 5.5 reports require the maximum level of logging enabled to collect the relevant data. Note that enabling maximum logging creates a large amount of data, which can affect server performance. Enable maximum logging only when needed and disable the logging when not in use

- To collect data for the Internet Mail by Day report, enable MSExchange IMC logging to maximum. To enable logging, complete steps 1 through 11 in the “To configure Exchange 5.5 to produce logging” procedure earlier in this chapter.
- To collect data for the Internet News by Day report, enable NNTP Service logging to maximum. To enable logging, complete steps 1 through 11 in the “To configure Exchange 5.5 to produce logging” procedure earlier in this chapter. At step 4, select the server protocols and, in the right pane, select the NNTP (News) settings.

The Microsoft Exchange 5.5 Management Pack module includes the Exchange Server Message Response Time processing rule group. This processing rule group features a script, **Throughput Response**, which allows you to verify the connectivity of your Exchange server and measure e-mail delivery time. This script sends e-mail to the Exchange server you specify, opens the destination mailbox to receive the e-mail, and finally creates numeric data that records the number of elapsed seconds from the time the e-mail was sent to the time the e-mail was received.

By collecting this performance data, you can graph and analyze the performance of your Exchange Server and be alerted to possible overloads or other availability issues. This processing rule group is disabled by default and must be manually enabled if you want to collect this data.

A timed event rule launches the event, so you can schedule the script to run at any set time interval. Agents run the script on Exchange servers. The script prevents mailbox overflow by deleting all the messages in the Inbox and by not saving copies of the sent messages in the Sent Items folder.

The Exchange 5.5 Management Pack Module also includes scripts to collect statistics about public folders and mailboxes. This data is used for generating Exchange Mailbox and Folder Sizes reports.

These scripts are launched by the timed event rules and require you to create specific mailboxes on each Exchange 5.5 server where you want the script to collect data.

▻ To configure Exchange computers for this performance data

1. Ensure the service account used for agents on Exchange servers has Exchange Administrator privileges.
2. Configure the Agent Manager property, Agent Service Account, to use the service account with Exchange Administrator privileges.
3. Using Exchange Administrator, configure the following mailboxes on all Exchange servers where you want the script to collect data. Ensure that the home server for the new mailboxes is set to the correct server.

   <*Site*>-<*Server*>-OnePointOperationsManager
   Used for logging on to MAPI for collecting public folder and mailbox statistics

   <*Site*>-<*Server*>-OnePointOperationsManagerIn
   Used by the **Throughput Response** script

   <*Site*>-<*Server*>-OnePointOperationsManagerOut
   Used by the **Throughput Response** script

   For example, for an Exchange server named ES1 in the site NORTHAMERICA, you would create the following mailboxes:

   ```
   NORTHAMERICA-ES1-OnePointOperationsManager
   NORTHAMERICA-ES1-OnePointOperationsManagerIn
   NORTHAMERICA-ES1-OnePointOperationsManagerOut
   ```

4. Using Exchange Administrator, associate these mailboxes with the agent service account as the primary Windows NT account.

Exchange Traffic Analysis reports summarize Exchange mail traffic patterns by message count and size using data collected from the Exchange Message Transfer Agent (MTA) log. To collect data for these reports enable Message Tracking on Exchange Server.

▻ To enable message tracking on Exchange 5.5 Server:

1. Log on to the Microsoft Exchange server as an Exchange Administrator.
2. Click **Exchange Administrator** in the Microsoft Exchange program folder.
3. Expand the **Organization** list, the **Site** list and select **Configuration**.
4. Select **MTA Site Configuration** in the results pane.
5. Click **Properties** on the **File** menu.
6. Select the **Enable message tracking** check box.
7. Select **Information Store Site** configuration.
8. Repeat steps 5 and 6.
9. Double-click **Connections** and select **Internet Mail Service**.
10. Repeat steps 5 and 6.

    Some of the rules that collect the data for the reports are disabled by default. You will have to enable those rules, as follows:

12. Open the MOM Administrator console.
13. Expand the following nodes: **Rules, Processing Rule Groups, Microsoft Exchange Server 5.5, Exchange Server 5.5, Exchange Shared Rules, Reporting for Exchange, and Event Processing Rules**.
14. In the right pane, enable all the report collection rules.

Default Notification Group

The default notification group for processing rule responses within the Exchange Management Pack module is Mail Administrators. For information about adding operators to this notification group, see the MOM Help.

Microsoft Proxy Server Management Pack Module

The following sections describe the purpose, features, configuration, and default notification group of the Microsoft Proxy Server Management Pack module.

Purpose

The Microsoft Proxy Server Management Pack module collects events generated by the Microsoft Proxy Server in Windows 2000. This Management Pack module ensures that this critical part of your Windows 2000 security is working correctly, and helps prevent costly service outages. By monitoring the events produced by the Microsoft Proxy Server, this Management Pack module increases the availability and security of your Windows 2000 network.

Features

The Microsoft Proxy Server Management Pack module collects the events the Microsoft Proxy Server places in the Windows 2000 System event logs. This Management Pack module highlights events that may indicate possible service outages, configuration problems, or security issues so that you can quickly take corrective or preventative actions. For example, this Management Pack module alerts you of the following conditions:

- Microsoft Proxy service has stopped, paused, or started
- Microsoft Proxy service failed to reach the network or the Internet host
- Microsoft Proxy service is out of available memory
- The Microsoft Proxy service connection to the server has been reset

Configuration

No special configuration for this Management Pack module is required.

Default Notification Group

The default notification group for processing rule responses within this Management Pack module is Web Administrators. For information about adding operators to this notification group, see the MOM Help.

Microsoft ISA Server Management Pack Module

The following sections describe the purpose, features, configuration, and default notification group of the Microsoft ISA Server 2000 Management Pack module.

Purpose

The Microsoft Internet Security and Acceleration Server 2000 Management Pack collects events generated by Microsoft ISA Server 2000 running on Windows 2000 Server and later. This Management Pack ensures that this critical part of your Windows 2000 security is working correctly, and helps prevent costly service outages. By monitoring the events produced by Microsoft ISA Server 2000, this Management Pack increases the availability and security of your Windows NT and Windows 2000 network.

Features

The Microsoft ISA Server 2000 Management Pack module collects the events Microsoft ISA Server 2000 places in the Windows 2000 event logs. This Management Pack module highlights events that may indicate possible service outages, configuration problems, or security issues, so that you can quickly take corrective or preventative actions. For example, this Management Pack module alerts you of the following critical conditions:

- Microsoft Proxy service has stopped, paused, or started
- Microsoft Proxy service failed to reach the network
- Internet host Microsoft Proxy service is out of available memory
- The Microsoft Proxy service connection to the server has been reset

Many Microsoft ISA Server 2000 Performance objects are being sampled. The default interval used for these measurements is 15 minutes. The data collected can be viewed from the following Microsoft ISA Server 2000 Views in MOM:

- Open Alerts for Firewall service
- Cache Performance
- Firewall Service Performance
- Total Dropped Packets
- Web Proxy Service Performance

Configuration

No special configuration is required for this Management Pack module.

By default, the ISA Rules that alert of ISA Informational Windows 2000 events are disabled. To turn them on, double-click each disabled rule and select **Enable**.

Default Notification Group

The default notification group for processing rule responses within this Management Pack module is Web Administrators. For information about adding operators to this notification group, see the MOM Help.

Microsoft Site Server 3.0 Management Pack Module

The following sections describe the purpose, features, configuration, and default notification group of the Microsoft Site Server 3.0 Management Pack module.

Purpose

The Microsoft Site Server 3.0 Management Pack module monitors the performance and availability of Microsoft Site Server version 3.0. This Management Pack module monitors the different elements of Microsoft Site Server, including List Builder, Membership Broker, Push, and Search for a complete Microsoft Site Server solution. By detecting critical events, this Management Pack module helps indicate and prevent possible Microsoft Site Server service outages.

The Microsoft Site Server 3.0 Management Pack module can play an important role in ensuring your Web site is available, and that all the functions you depend on are working correctly. You can use this Management Pack module to provide a high level of customer responsiveness. Increasing the availability and performance of Microsoft Site Server 3.0, this Management Pack module reduces your cost of ownership by enabling proactive management.

Features

The Microsoft Site Server 3.0 Management Pack module monitors events placed by Microsoft Site Server 3.0 and its services in the Application and System event logs. This Management Pack module highlights events that might indicate possible service outages, configuration problems, or security issues so that you can quickly take corrective or preventative actions. It allows you to proactively manage your Microsoft Site Server configuration and avoid costly service outages. For example, this Management Pack module alerts you of the following critical conditions:

- Remote networks are unavailable
- Failure of Site Server authentication, indicating a security issue
- Resource issues affecting service levels
- Project or content index files are corrupt

Note

Microsoft Site Server version 3.0 is supported only on Windows 2000 with Site Server 3.0 Service Pack 4 installed.

Configuration

No special configuration for this Management Pack module is required.

Default Notification Group

The default notification group for processing rule responses within this Management Pack module is Web Administrators. For information about adding operators to this notification group, see the MOM Help.

Microsoft SNA Server 4.0 Management Pack Module

The following sections describe the purpose, features, configuration, and default notification group of the Microsoft SNA Server 4.0 Management Pack module.

Purpose

The Microsoft SNA Server 4.0 Management Pack module collects events generated by Microsoft SNA Server version 4.0 in Windows 2000. This Management Pack module ensures that this critical gateway application is working correctly, and helps prevent costly service outages. By monitoring the events produced by Microsoft SNA Server 4.0, this Management Pack module increases the security and availability of your Windows 2000 network.

Features

The Microsoft SNA Server 4.0 Management Pack module collects the events generated by Microsoft SNA Server 4.0 running on Windows 2000 Application event logs. This Management Pack module highlights events that may indicate possible service outages, configuration problems, or security issues so you can quickly take corrective or preventative actions. For example, this Management Pack module alerts you of the following critical conditions:

- Failures in starting and stopping the SNA server
- Resynchronization service failures
- Too many network resources active, indicating service availability issues
- LAN connection failures
- Host connection failures

Note

SNA 4.0 is supported on Windows NT 4 with Service Pack 6, and Windows 2000 with SNA 4.0 Service Pack 4 installed. It is not supported on other operating systems.

Configuration

No special configuration for this Management Pack module is required.

Default Notification Group

The default notification group for processing rule responses within this Management Pack module is Network Administrators. For information about adding operators to this notification group, see Help.

Microsoft Host Integration Server 2000 Management Pack Module

The following sections describe the purpose, features, configuration, and default notification group of the Microsoft Host Integration Server 2000 Management Pack module.

Purpose

The Microsoft Host Integration Server 2000 Management Pack module collects events generated by Microsoft Host Integration Server 2000 and its services in Windows 2000 or later. This Management Pack module ensures that Host Integration Server 2000 and its services are working correctly, and helps prevent costly service outages. By monitoring the events produced by the Host Integration Server 2000, this Management Pack module increases the security and availability of your Windows 2000 network.

Features

The Microsoft Host Integration Server 2000 Management Pack module collects events Microsoft Host Integration Server 2000 places in the Windows 2000 Application event logs. This Management Pack module highlights events that might indicate possible service outages, configuration problems, or security issues so you can quickly take corrective or preventative actions. For example, this Management Pack module alerts you of the following critical conditions:

- Failures starting and stopping the Host Integration Server 2000 components
- Resynchronization service failures
- Too many network resources active, indicating service availability issues
- LAN connection failures
- Host connection failures due to service outages or other host-related issues
- Configuration replication failures between Host Integration 2000 servers

The Host Integration 2000 Management Pack supports monitoring of events, services and performance counters for multiple instances of Host Integration Server 2000.

Note

Host Integration Server 2000 is supported only on Windows 2000 and later.

Configuration

No special configuration for this Management Pack module is required.

Default Notification Group

The default notification group for processing rule responses within this Management Pack module is Network Administrators. For information about adding operators to this notification group, see the MOM Help.

Microsoft SQL Server™ Management Pack Module

The following sections describe the purpose, features, configuration, and default notification group of the Microsoft SQL Server Management Pack module.

Purpose

The Microsoft SQL Server Management Pack module monitors SQL Server version 7 and SQL Server 2000. By detecting, alerting on, and automatically responding to critical events, this Management Pack module helps indicate, correct, and prevent possible service outages or configuration problems.

With the embedded expertise in the SQL Server Management Pack module, you can proactively manage SQL Server, and identify issues before they become critical. This Management Pack module increases the security, availability, and performance of SQL Server.

Features

This Management Pack module highlights events that might indicate possible service outages or configuration problems, so you can quickly take corrective or preventative actions. For example, this Management Pack module alerts you of the following critical conditions:

- Deadlock type problems
- Blocking Issues
- Replication Failure Errors
- Log Shipping Related errors
- SQL Server becomes unavailable
- SQL Server can no longer accept connections
- The SQL Server process crashes
- SQL Server cannot allocate memory for normal operations

The SQL Server 2000 Management Pack supports monitoring of events, services and performance counters for multiple instances of SQL Server 2000. In addition, this Management Pack also includes scripts to measure SQL Server availability.

Reports

The following is a list of available SQL Server reports.

- SQL Server Capacity Planning reports summarize SQL Server usage, such as backup device and user connections, and help you plan for current and future capacity needs.
- SQL Server Operations reports summarize critical SQL Server operation-related events.
- SQL Server Performance Analysis reports graph SQL Server performance counters and help you analyze such areas as memory, replication, and lock performance.

All reports work for SQL Server 7.0 and SQL Server 2000, including support for multiple instances of SQL Server 2000. For a more detailed description of all SQL Server reports, see the **Report Descriptions** topic in the MOM Help.

Configuration

No special configuration for this Management Pack module is required.

By default, the SQL Server 2000 Management Pack module does not collect SQL Server performance counters from all instances of SQL Server. Collection of performance counters from multiple instances of SQL Server 2000 is done through the use of scripts. There is one script for each SQL Server 2000 object. Each script collects all SQL Server 2000 performance counters from all SQL Server 2000 instances within a specific object. To enable collection of specific counters, you need to determine which object contains the specific counters and disable the script for that particular object. Below is the list of scripts and the performance counters that each of the scripts collect.

SQL Server Multiple Instance Perf Data for Access Methods
Collects all counters within the **AccessMethods** object

SQL Server Multiple Instance Perf Data for BufferManager
Collects all counters within the **BufferManager object**

SQL Server Multiple Instance Perf Data for Backup Device
Collects all counters within the **BackupDevice** object

SQL Server Multiple Instance Perf Data for CacheManager
Collects all counters within the **CacheManager object**

SQL Server Multiple Instance Perf Data for Databases
Collects all counters within the **Databases object**

SQL Server Multiple Instance Perf Data for GeneralStatistics
Collects all counters within the **GeneralStatistics object**

SQL Server Multiple Instance Perf Data for Latches
Collects all counters within the **Latches object**

SQL Server Multiple Instance Perf Data for Locks
Collects all counters within the **Locks object**

SQL Server Multiple Instance Perf Data for memoryManager
Collects all counters within the **MemoryManager object**

SQL Server Multiple Instance Perf Data for ReplicationAgents
Collects all counters within the **ReplicationAgents object**

SQL Server Multiple Instance Perf Data for ReplicationDist
Collects all counters within the **ReplicationDist object**

SQL Server Multiple Instance Perf Data for ReplicationLogReader
Collects all counters within the **ReplicationLogReader object**

SQL Server Multiple Instance Perf Data for ReplicationMerge
Collects all counters within the **ReplicationMerge object**

SQL Server Multiple Instance Perf Data for ReplicationSnapShot
Collects all counters within the **ReplicationSnapShot object**

SQL Server Multiple Instance Perf Data for SQLStatistics
Collects all counters within the **SQLStatistics object**

SQL Server Multiple Instance Perf Data for UserSettable
Collects all counters within the **UserSettable object**

Default Notification Group

The default notification group for processing rule responses within this Management Pack module is Database Administrators. For information about adding operators to this notification group, see the MOM Help.

Microsoft Application Center 2000 Management Pack Module

The following sections describe the purpose, features, configuration, and default notification group of the Microsoft Application Center 2000 Management Pack module.

Purpose

The Microsoft Application Center 2000 Management Pack collects events generated by Microsoft Application Center 2000 servers running on Windows 2000 server and later. This Management Pack module helps ensure that your Web applications, and the clusters they belong to, are achieving mission-critical availability, and are working optimally. By monitoring the events produced by Application Center 2000, this Management Pack module increases the availability, performance, and security of your Windows 2000 network.

Features

The Microsoft Application Center 2000 Management Pack module collects the WMI events created by Microsoft Application Center 2000. This Management Pack module highlights events that might indicate possible service outages, configuration problems, or security issues, so that you can quickly take corrective or preventative actions. Some of the critical conditions this Management Pack module will alert you to include:

- Clustering
- Cluster control unavailable
- Cluster controller errors and failures
- Cluster name resolution errors and failures
- Cluster tome synchronization errors and failures
- Monitoring
- Event Logging errors and failures
- Event Logging Agent errors and failures
- Performance Logging and Counter errors and failures
- Replication
- Replication Authentication errors and failures
- Replication HTTP connection errors and failures
- Object Replication errors and failures
- Application Replication errors and failures
- Request Forwarding
- Request Forwarding services unavailable
- Request Forwarding thread pool errors and failures

Many Microsoft Application Center 2000 **Request Forwarding** performance objects are also being sampled. The default interval used for these measurements is 15 minutes. The following are several examples of the data you can collect and view from the Application Center 2000 views in MOM:

- Total Failed Requests
- Publishing Requests
- Total Requests
- Application Center Administration Requests
- Coherent Session Requests

Configuration

No special configuration is required for this Management Pack module.

By default, the Application Center 2000 rules for informational events are disabled and are not set to generate an alert. To turn them on, double-click each disabled rule, and then select **Enable**.

Default Notification Group

The default notification group for processing rule responses within this Management Pack module is Application Center administrators. For information about adding operators to this notification group, see the MOM Help.