

Microsoft Operations Manager 2005 Field Guide



Andy Dominey
Garry Meaburn

Apress®

Microsoft Operations Manager 2005 Field Guide

Copyright © 2006 by Andy Dominey and Garry Meaburn

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the copyright owner and the publisher.

ISBN-13 (pbk): 978-1-59059-709-5

ISBN-10 (pbk): 1-59059-709-5

Printed and bound in the United States of America 9 8 7 6 5 4 3 2 1

Trademarked names may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, we use the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

Lead Editor: Jonathan Gennick

Technical Reviewer: Judith Myerson

Editorial Board: Steve Anglin, Ewan Buckingham, Gary Cornell, Jason Gilmore,

Jonathan Gennick, Jonathan Hassell, James Huddleston, Chris Mills,

Matthew Moodie, Dominic Shakeshaft, Jim Sumser, Keir Thomas, Matt Wade

Project Manager: Richard Dal Porto

Copy Edit Manager: Nicole Flores

Copy Editor: Damon Larson

Assistant Production Director: Kari Brooks-Copony

Senior Production Editor: Laura Cheu

Compositor: Linda Weidemann, Wolf Creek Press

Proofreader: Elizabeth Berry

Indexer: Toma Mulligan

Artist: Kinetic Publishing Services, LLC

Cover Designer: Kurt Krames

Manufacturing Director: Tom Debolski

Distributed to the book trade worldwide by Springer-Verlag New York, Inc.,
233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER,
fax 201-348-4505, e-mail orders-ny@springer-sbm.com, or visit
<http://www.springeronline.com>.

For information on translations, please contact Apress directly at 2560 Ninth Street,
Suite 219, Berkeley, CA 94710. Phone 510-549-5930, fax 510-549-5939, e-mail
info@apress.com, or visit <http://www.apress.com>.

The information in this book is distributed on an “as is” basis, without warranty. Although every precaution has been taken in the preparation of this work, neither the author(s) nor Apress shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.



Management Pack Installation and Configuration

Management packs are one of the core components of your MOM infrastructure. Without them, no monitoring would take place, as MOM would not know what to look for. One of the most common mistakes made is the installation of more management packs than are actually required. The more management packs that are installed, the more alerts there are to tune and the more data there is to be collected from the agents.

The aim of this chapter is to show you the minimum management pack installation for monitoring your systems, and how you should manage changes and/or introduce new management packs into your MOM environment. It will cover the following areas:

- Management pack definition
- Management pack installation best practices
- Management pack requirements to monitor various Microsoft products
- The rules assigned to an agent

What is a Management Pack?

A management pack is collection of configuration settings that allow you to monitor a system. Management packs are available from Microsoft and third-party vendors. You can also create your own packs for your specific requirements.

A management pack can consist of all or a selection of the following configuration settings, depending on the complexity of the management pack:

- Rules
- Schemas

- Attributes to be collected for computer groups
- Computer group rules
- Relationships
- Provider instances
- Rule groups
- Views
- Reports in a separate XML file
- Knowledge bases
- Tasks
- Notification groups
- Scripts
- Topology diagram definitions

Computer Groups

Computer groups are groups of computers that are based on attributes or manually selected. An example is the Microsoft Windows 2003 Servers computer group, which is created when you install Microsoft Windows Server Base Operating Systems Management Pack for MOM 2005. This will contain all the computers that have Windows 2003 installed, and allows you to use computer groups for the following:

- Rule targeting
- Rollup views
- Console scopes
- Computer group views
- Rule override targeting

Computer groups can be nested—containing other computer groups—and a computer group or computer can be a member of multiple computer groups. The membership of the computer groups can either be dynamic or static. Group membership can be defined by wildcard or regular expression on a domain and computer name, based on attributes (e.g., a registry key or value) or the inclusion of another computer group. The group membership is calculated continuously as discovery data is updated for the agent. Static membership is defined by the MOM administrator using a list of computers that you want to include or exclude from the group.

Note One important difference between MOM 2000 and MOM 2005 is that in MOM 2000, the management console showed which computers had been discovered and were populated in the computer group. In MOM 2005, the discovered servers do not show up in the Administrator Console—they are instead displayed in the Operator Console.

Management Pack Installation Best Practices

When a management pack is imported, in most instances the pack will include computer groups that have attribute-based membership criteria and enabled rules. Once the management pack is installed, it becomes active. The following subsections outline some best practices for installing new management packs. Follow these practices to help avoid any adverse impact when installing new packs.

Creating a Sandbox Environment

Using either spare hardware or a virtual server environment, you can create a sandbox environment that is isolated from the production environment. This will be used to test the initial install of a management pack and the creation of new rules. When possible, this should contain the main components of your production environment (e.g., an Exchange server and a domain controller).

To start initial tuning of the management pack, you should do the following:

1. Carry out any post-installation configuration requirements.
2. Check that the installation of the new management pack has not impacted any of the existing management pack installations (e.g., after installing the first release of the Availability management pack, it accidentally deletes a number of the Exchange computer groups).

After you complete the steps, you should export the management packs into a staging environment (which is our topic for the next section). You should document any changes to the management pack.

Creating a Preproduction Staging Environment

Creating a preproduction staging environment will allow you to mirror the main components of your production environment and also contain all the

live management packs. This staging environment can be made up of virtual machines and multihomed machines from your production environment. The deployment to the multihomed agents should only take place once you have tuned the management pack.

If the main management pack is in place, do the following:

1. Create a management server performance baseline before the new management pack is installed. See Chapter 4 for details on how to do this.
2. Import the new management pack.
3. Start a new management server performance baseline.
4. Compare the before and after baselines to ensure that the new management pack does not overload the management server.
5. Do the same for the agent performance baseline to ensure that the agent's performance is not impacted.
6. Analyze the alerts received from the new management pack. You should check the following:
 - That only valid alerts are being received—not alerts generated by misconfigurations (e.g., incorrect access rights).
 - That thresholds have been tuned to match your environment and alerts are being generated accordingly.
 - That the volume of alerts is at an acceptable level. If a management pack is “noisy,” then operations teams may ignore the alerts that are being generated, and event storms may happen.

Tip The Alert Tuning Solution Accelerator (which you can download from <http://go.microsoft.com/fwlink/?LinkId=33861&clcid=0x409>) has a number of reports that can be used to analyze the alerts generated by the management pack.

After you carry out most of the tuning, you should deploy the management pack to the multihomed agents. This will allow you to check the management pack against your production environment in a controlled manner. When possible, you should test at least two multihomed agents: one on a well-connected site and one on a site with poor network links. This method of testing will highlight alerts that are triggered by slow networks. You should use rule overrides whenever possible in these scenarios to configure the alert thresholds for well-connected and poorly connected agents. You should be ready to export the management pack into your production system.

You should document any changes to the management pack, and you should update this documentation every time you make changes.

Note Override targets are not exported when you export a management pack. To get around this issue, either document the overrides that have been configured and recreate them in the production system, or use the `Overrides.exe` file, which is available in the MOM 2005 SDK. Using this tool, you can export the management pack, and then export the override targets using the `Overrides /dump filename` command. You can then import the management pack and the override targets into the production system by using the `Overrides /create filename` command.

Best Practices for Customizing Management Pack Rules

A typical MOM installation can have over 1,000 management pack rules. Typically, you will need to change the default configuration on a number of these management pack rules to meet your needs. The issue is that when you import a new version of a particular management pack, you may lose your configurations. Even if you select the merge rule, only the enabled/disabled flag and the company knowledge entries are retained.

Each rule has a unique rule GUID (globally unique identifier), so renaming the changed rule will not overcome this issue during the import. The rule will be overwritten, as it is identified by GUID rather than name.

The following process should be followed to ensure that the impact of importing updated management packs is reduced:

1. Create a new rule group based on the management pack name from which the rules are going to be copied (e.g., *Company Name* - Microsoft Operations Manager). If necessary, create any child rule groups based on the names of the original child rule group (e.g., *Company Name* - Operations Manager 2005). This allows you to easily see where the rules have come from, and also allow the rule targeting at the child rule group level as required.
2. Copy the rule that you are going to modify into this new structure, and then disable the original rule.
3. Change the name of the newly copied-over rule back to the original name, as “Copy of” will have been appended to the rule’s name.

4. Populate the Knowledge Base entry in this rule, as it will be empty, and isn't copied over by default. To populate this field, you have two options: either share knowledge between two rules or simply copy and paste the Knowledge Base entry from the original rule into the company knowledge section of the new rule.
5. Once all rules have been copied over, associate the parent and child rule groups with the correct computer groups. You must match this association with the association of the original rule groups to ensure that the rules are applied to the correct agents.

Figure 3-1 shows an example of the configuration rules that you will have modified in the MOM rule group.

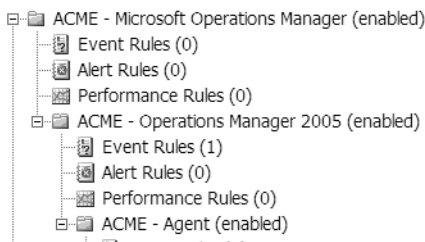


Figure 3-1. *Modified rule group*

This process may seem time-consuming, but in reality, the number of rules that you will customize will be relatively few. If you customize the rules in their original locations, you can avoid the difficulties of trying to manage the import of an updated management pack into your environment.

Management Pack Requirements

The aim of this section is to provide information on the management packs that should be installed to monitor the following:

- Active Directory
- Exchange
- Internet Information Services (IIS)
- Windows clusters
- Simple Network Management Protocol (SNMP)
- SQL 2000 and 2005

The Management Pack and Utilities catalog, which provides further information, is located at www.microsoft.com/management/mma/catalog.aspx. We will give more details later in this section.

Active Directory

Active Directory is the backbone of most companies' Windows infrastructures. It is therefore critical that proactive management is carried out to avoid business outages. The main components that need to be monitored are as follows:

- OS (Windows 2000 and Windows 2003)
- Distributed file system (DFS)
- File replication service (FRS)
- Domain name system (DNS)
- Group policy (GPO)
- Server hardware
- Directory services

Install the following management packs to monitor the Active Directory server environment:

- Active Directory (AD) Management Pack for MOM 2005
- Group Policy Management Pack for MOM
- Microsoft Windows Distributed File System Service Management Pack for Microsoft Operations Manager 2005
- Microsoft Windows Server Base Operating Systems Management Pack for Microsoft Operations Manager 2005
- Domain Name Service (DNS) Management Pack for MOM 2005
- Microsoft Windows File Replication Service Management Pack for Microsoft Operations Manager 2005

Depending on the hardware used to host the Active Directory environment, one or more of the following management packs should be installed:

- HP Server Management Packs for MOM 2005
- Dell Management Pack for MOM 2005
- IBM Director 5.10 (for integration of IBM Director with MOM 2005)

Note The File Replication Service management pack relies heavily on having Ultrasound installed in your environment. A MOM agent should be installed on the server that hosts the Ultrasound installation. You should ensure that your process for managing FRS alerts also includes resolving the alerts in Ultrasound, as the management pack does not send alert status changes back to the Ultrasound server.

Exchange Servers

Since businesses have become dependent on e-mail, many processes and procedures are integrated with the environment of sending and receiving e-mail. Therefore, it is critical that the messaging environment is monitored closely. The messaging environment is also one of those areas on which managers like to have reports and statistics for service level agreement (SLA) reporting. In this section, we will focus on Exchange 2000/2003, as Exchange 5.5 support ended on December 31, 2005.

Install the following management packs to monitor an Exchange Server environment:

- Microsoft Exchange Server Management Pack for MOM 2005
- Microsoft Exchange Server Best Practices Analyzer Management Pack for Microsoft Operations Manager 2005
- Microsoft Operations Manager 2005 SLA Scorecard for Exchange
- Microsoft Availability Reporting Management Pack for Microsoft Operations Manager 2005
- Microsoft Windows Server Base Operating Systems Management Pack for Microsoft Operations Manager 2005

Depending on the hardware that is used to host the Exchange environment, one or more of the following management packs should be installed:

- HP Server Management Packs for MOM 2005
- Dell Management Pack for MOM 2005
- IBM Director 5.10 (for integration of IBM Director with MOM 2005)

Note If you install Microsoft Operations Manager 2005 SLA Scorecard for Exchange, there is a misconfigured rule. The Service Control Manager event for the Service Stopped/Started rule should have the This Rule Generates Alert check box unchecked—otherwise it will generate an alert for every event ID 7036. The rule should be just a collection rule, not an alert-generating rule. If it is not unchecked, your Operator Console will be flooded with critical alerts.

You can also utilize some of the features of the Active Directory management pack to ensure that the Active Directory environment that has to service the Exchange environment is responding as expected. This can be achieved when you add the Exchange servers into the Active Directory Client Side Monitoring computer group. This allows the Exchange server to test whether Active Directory is available by the following:

- Pinging (using both Internet Control Message Protocol [ICMP] and Lightweight Directory Access Protocol [LDAP])
- Searching Active Directory
- Confirming that a sufficient number of global catalog servers are available
- Detecting primary domain controller PDC availability and responsiveness

If you are concerned about installing extra components on the Exchange servers, you can add a server that is on the same physical site as the Exchange server, and this server will carry out the checks.

IIS

Web sites are utilized heavily by businesses now. A web site may be the first encounter a potential new customer has with a company. It is important, then, that any issues that could potentially cause downtime or poor performance—such as broken links, unavailable sites, and security breaches—are alerted on.

Install the following management packs to monitor the IIS server environment:

- Internet Information Server (IIS) Management Pack for MOM 2005
- Microsoft Web Sites and Services Management Pack for MOM 2005
- Microsoft Windows Server Base Operating Systems Management Pack for Microsoft Operations Manager 2005

Depending on the hardware that is used to host the web servers, one or more of the following management packs should be installed:

- HP Server Management Packs for MOM 2005
- Dell Management Pack for MOM 2005
- IBM Director 5.10 (for integration of IBM Director with MOM 2005)

If you wish to monitor the Live Communication Server (LCS) web component, then also install the Office Communicator Web Access Management Pack for MOM 2005.

You should pay particular attention to the Web Sites and Services management pack, as you will be able to closely monitor the availability and functionality of the web site or web service. Out of the box, this management pack does not contain any preconfigured rules that allow you to monitor a web application or web service. You must take time to configure the management pack to meet your requirements. The following link has more information on the management pack: www.microsoft.com/technet/prodtechnol/mom/mom2005/maintain/momwssmpguide_3.msp.

Note If you don't have the current IIS management pack installed, ensure that you disable the following rules:

Security: Error 401: "Access Denied" Error - Alert

Security: Error 401: "Access Denied" - Event Consolidation

It has been known for the IIS management pack to randomly add IP address and domain name restrictions to all web sites on the local computer. These rules must be disabled for IIS 5 and 6.

Windows Clusters

Clustering allows the delivery of higher levels of service and availability so that you can ensure that the clustered environment meets the business needs. For this reason, you need to carefully monitor these clusters. Install the following management packs to monitor the cluster environment:

- Server Clusters Management Pack for MOM 2005
- Microsoft Windows Server Base Operating Systems Management Pack for Microsoft Operations Manager 2005

Depending on the hardware that is used to host the clusters, one or more of the following management packs should be installed:

- HP Server Management Packs for MOM 2005
- Dell Management Pack for MOM 2005
- IBM Director 5.10 (for integration of IBM Director with MOM 2005)

These management packs will monitor the core components of the cluster installation. Additional management packs should be installed based on the applications that will be hosted on the cluster (e.g., Exchange or SQL).

Once you have installed the management pack and discovered the cluster, you need to go to the Windows Server clusters in the Administrator Console. Right-click them and select Start Managing. It is also recommended that you disable event log replication to avoid generating duplicate alerts. If you decide to leave event log replication enabled, then you need to allow the agent proxying for the cluster nodes; otherwise, you may receive security alerts in MOM. You can disable event log replication via a built-in task in the MOM Operator Console, or by entering **EnableEventLogReplication=0** at the command prompt on a cluster node.

The use of clusters in your environment may have an impact on some of the management packs, such as the Microsoft Operations Manager 2005 SLA Scorecard for Exchange, which currently does not support clusters.

SNMP

MOM 2005 can monitor SNMP traps. This allows you to configure MOM to monitor non-Windows systems (e.g., UPS, routers, etc.). You are required to make the configurations rather than just upload a management pack. The following example will show how to monitor the HP StorageWorks Reference Information Storage System (RISS) via SNMP. In this example, the RISS has only three traps that we are interested in. These are described in Table 3-1.

Table 3-1. *SNMP Traps*

Trap ID	Description
1.3.6.1.4.1.14701.6.6.1	A notification will be sent if any SmartCell goes into the dead state.
1.3.6.1.4.1.14701.6.6.2	A notification will be sent if any host is down.
1.3.6.1.4.1.14701.6.6.3	A notification will be sent if any service listed in PCC has the state CRITICAL.

The RISS system does not come with any management information base (MIB), so the translations have to be done inside MOM. To set up MOM to receive SNMP traps, you need to set up the management server and the SNMP rule group.

Setting Up the Management Server to Collect SNMP Traps

It takes five steps to set up the management server to collect SNMP traps. The following sections show you how you perform them.

Step One

To ensure that the SNMP service and WMI SNMP provider are installed on the management server, do the following:

1. Open Add/Remove Programs.
2. Click the Add/Remove Windows Components button.
3. Select Management and Monitoring Tools from the Windows Components dialog.
4. Click the Details button, and install SNMP and the WMI SNMP Provider.

Note On Windows 2000, you can find the WMI SNMP Provider on the Windows 2000 CD, in a file called WBEMSNMP.EXE.

Step Two

To configure the SNMP service to accept traps, do the following:

1. Go to Computer Management ► Services and Applications, and double-click the SNMP service in the Services window.
2. In the SNMP Service Properties window, click the Security tab.
3. Ensure that the Accept SNMP packets from any host check box is checked, as shown in Figure 3-2.

Note SNMP is insecure, so when possible you should rename the community name to something other than the default PUBLIC.

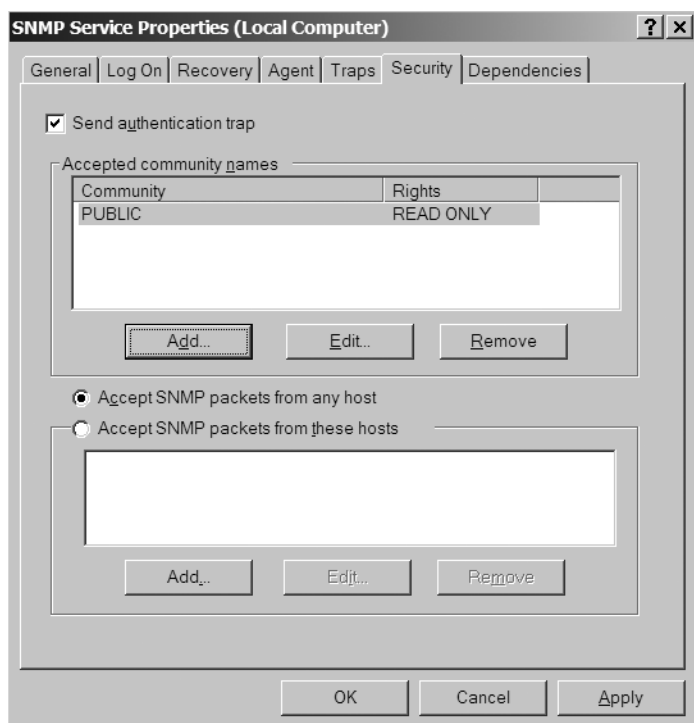


Figure 3-2. *The SNMP Service Properties window*

4. On the General tab, you should configure the service to start up automatically. Once you've done that, click Apply, and then click OK.
5. Go to the SNMP Trap service in the service window and configure the startup to automatic.

Step Three

In the MOM Administrator Console, create a new computer group (called, for example, SNMP Server) and the management server(s) for this group.

Step Four

Create a new rule group following your standard naming convention (e.g., ACME SNMP).

Step Five

Associate the SNMP rule group to the computer group that you have created.

Setting Up an SNMP Rule Group

It takes eight steps to create an SNMP collection event. This is how you do it:

1. Under ACME SNMP in the MOM Administrator Console, right-click Event Rules. From the pop-up menu, select Create Event Rule. This is shown in Figure 3-3.

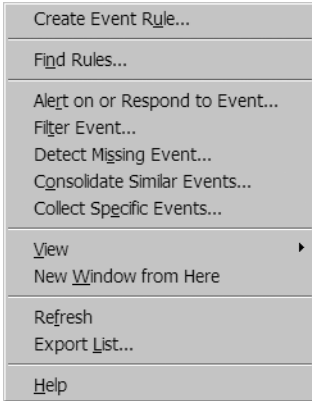


Figure 3-3. *Selecting the Create Event Rule option*

2. In the Select Event Rule Type window, select Collect Specific Events (Collection), and then click Next. This is shown in Figure 3-4.

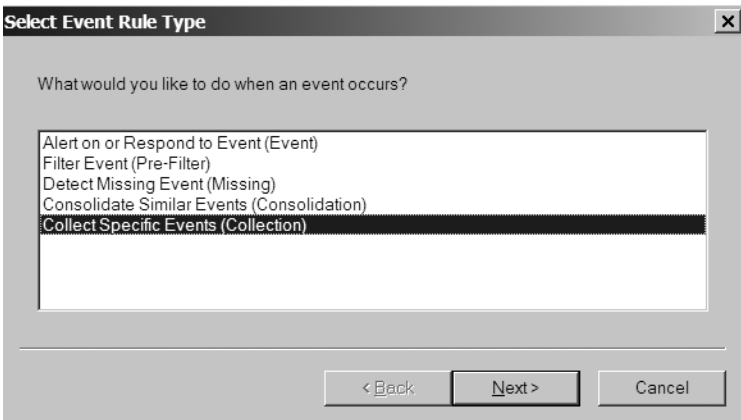


Figure 3-4. *Selecting Collect Specific Events (Collection)*

3. In the Collection Rule Properties - Data Provider window, select SNMP Extended Trap Catcher as the provider, and then click Next. This is shown in Figure 3-5.

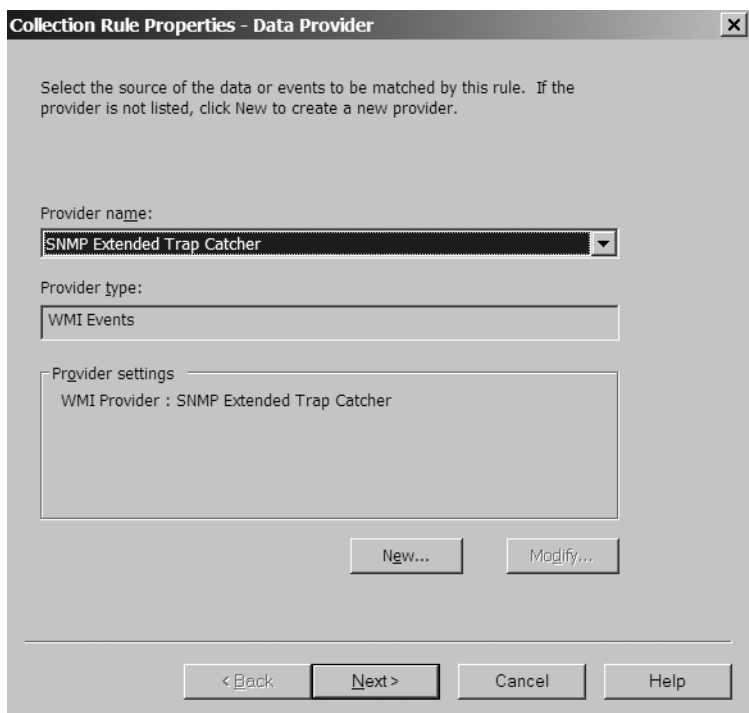


Figure 3-5. *Selecting the provider name*

4. In the Collection Rule Properties - Criteria window, accept the default settings, for which all the Match events boxes are unchecked (as shown in Figure 3-6). Click Next.

Collection Rule Properties - Criteria

Select the properties of events that you would like to match.

Match events

☐ from source

☐ with event id

☐ of type

☐ with description

Criteria description

Advanced...

< Back Next > Cancel Help

Figure 3-6. *Configuring the criteria*

5. In the Collection Rule Properties - Parameter Storage window, select Store all event parameters, and then click Next. This is shown in Figure 3-7.

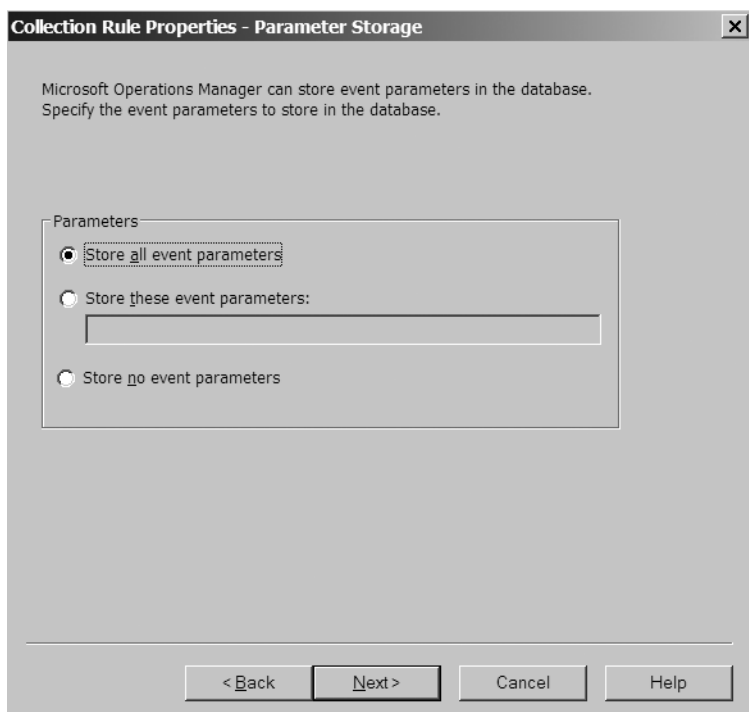


Figure 3-7. *The Parameter Storage window*

6. From the drop-down menu in the Collection Rule Properties - Schedule window, Select Always process data, and then click Next. This is shown in Figure 3-8.

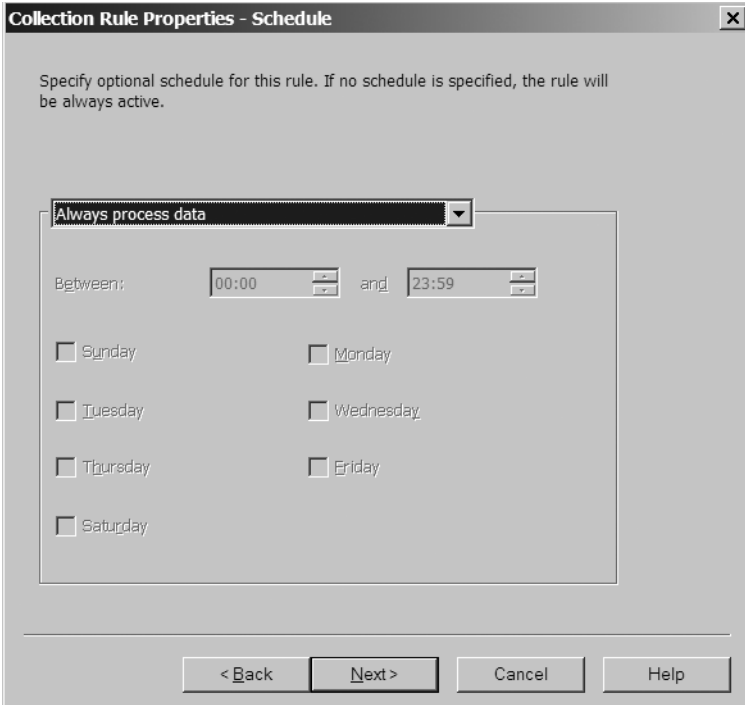


Figure 3-8. *Schedule to process data*

7. In the Collection Rule Properties - Knowledge Base window, enter the knowledge base details on a collection rule. After you have finished entering the details, click Next. This is shown in Figure 3-9.

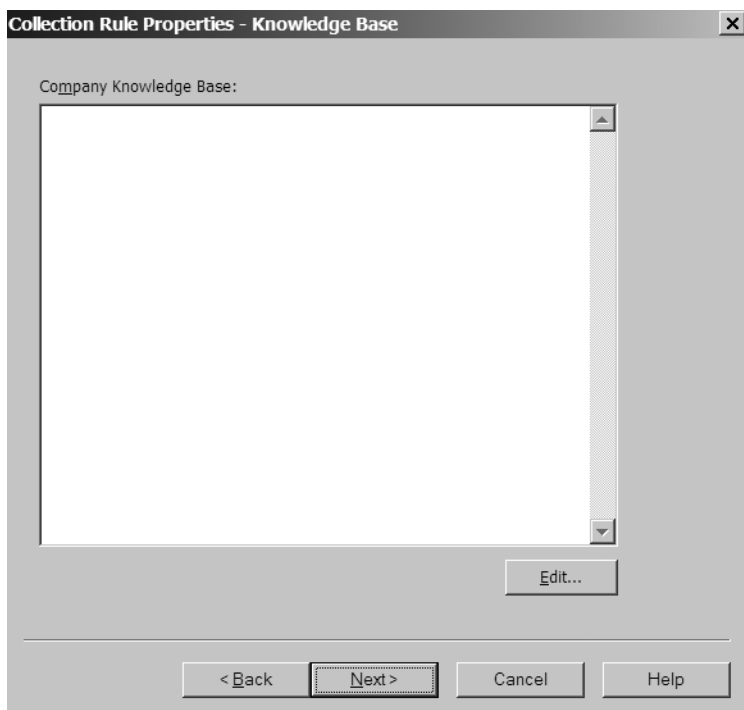


Figure 3-9. *The Knowledge Base window*

8. In the Collection Rule Properties - General window, enter a rule name. Make sure that the rule is enabled. Do not enable rule-disable overrides for this rule. Click Finish. This is shown in Figure 3-10.

Collection Rule Properties - General

Rule Name:

Rule action:

Rule GUID:

☒ This rule is enabled

☐ Enable rule-disable overrides for this rule

Override Name:

No override criteria have been set.

Note: Changing the override name assigns a new override to this rule property. Override criteria set for the previous override name will no longer apply to this rule.

Figure 3-10. *The General window*

Setting Up Alerts for SNMP Traps

It takes 12 steps to set up alerts for SNMP traps. This is how you do them:

1. In the Administrator Console, expand the ACME SNMP rule group and right-click Event Rules. From the pop-up menu, select the Alert on or Respond to Event rule. This is shown in Figure 3-11.
2. In the Event Rule Properties - Data Provider window, select SNMP Extended Trap Catcher as the provider, and then click Next. This is shown in Figure 3-12.
3. In the Event Rule Properties - Criteria window, click Advanced.

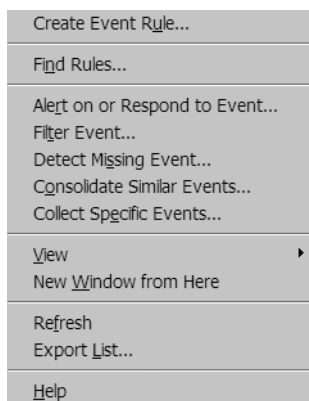


Figure 3-11. *Selecting the Alert on or Respond to Event rule*

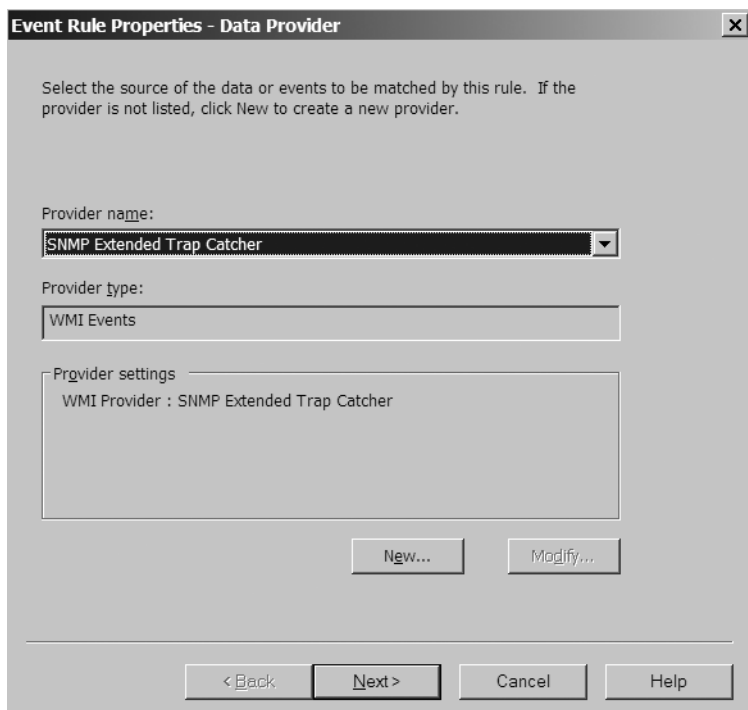


Figure 3-12. *Selecting the data provider*

4. In the Advanced Criteria window, configure the following, and click Add to List. This is shown in Figure 3-13.
 - *Field*: Description
 - *Condition*: contains substring
 - *Value*: 1.3.6.1.4.1.14701.6.6.2
5. Configure the following, click Add to List, and then click Close. This is shown in Figure 3-13.
 - *Field*: Parameter 17
 - *Condition*: contains substring
 - *Value*: DOWN

Advanced Criteria

Process only data that matches all these criteria:

Field	Condition	Value
Description	contains substring	1.3.6.1.4.1.14701.6.6.2
Parameter 17	contains substring	DOWN

Define more criteria:

Field: Condition: Value:

Buttons: Close, Help, Remove, Add to List, < Back, Next >, Cancel, Help

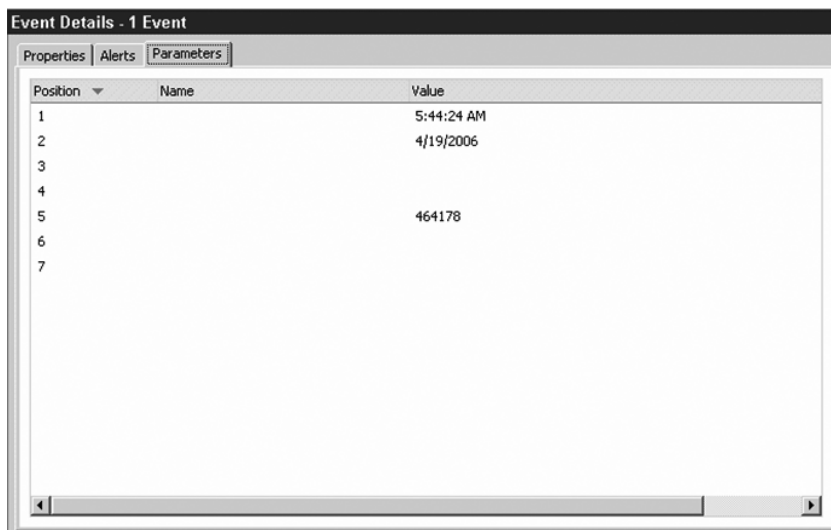
Figure 3-13. *The Advanced Criteria window*

6. In the Event Rule Properties - Criteria window, click Next.
7. In the Schedule window, select Always process data.
8. In the Event Rule Properties - Alert window, check This Rule Generate Alerts, and set the alert severity to critical. In the Description field, enter **RISS host \$Parameter 17\$,** and then click Next.

9. In the Event Rule Properties - Alert Suppression window, uncheck Suppress Duplicate Alerts, and then click Next.
10. In the Event Rule Properties - Responses window, click Next.
11. In the Event Rule Properties - Knowledge Base window, enter the company details, and then click next.
12. In the Event Rule Properties - General window, enter a rule name. Ensure that the rule is enabled. Do not enable rule-disable overrides for this rule. Click Finish.

This information provides the basic steps to configure an alert for the SNMP trap 1.3.6.1.4.1.14701.6.6.2, with a status that the host is down.

You can alter this process to match any SNMP traps that you want to capture in MOM. The parameters for the SNMP traps can be worked out by looking at the events in the Operator Console, and then clicking the Parameters tab. In Figure 3-14, the position number represents the parameter numbers on the alert in the Advanced Criteria window.



Position	Name	Value
1		5:44:24 AM
2		4/19/2006
3		
4		
5		464178
6		
7		

Figure 3-14. *Example of event parameters*

The previous example did not import MIBs, so the meaning of the alert had to be manually added to the Description field. Otherwise, the alert would not be very meaningful to the operations team. If the device that you are going to monitor has MIBs available, it is possible for you to import the MIBs into MOM. This will make it easier to translate the SNMP trap into an

alert that you can understand. You can also use the SM12SMIR utility to import the MIBs. This will load the MIB information into the WMI `\\.\root\snmp\smir` namespace and provide SNMP trap translations. Otherwise, you will just receive object identifiers, which are basically strings of numbers (e.g., 1.3.6.1.4.1.9.9.163.2.0.1) and possibly a status value.

Identifying the Rules Assigned to an Agent

When troubleshooting an agent, it is often important to see what rules are assigned to it. There are numerous ways of identifying what rules are assigned to an agent—the following section shows you how you do it.

The Resultant Set of Rules (RSOR) Utility

The resource kit includes the RSOR utility, which will generate a plain text file showing the set of rules that would be deployed to an agent. The syntax is `RSOR.exe <MOMDBServer> <TargetAgent>`. The output is then placed in `C:\ResultantSetOfRules`. If your operations database is a SQL instance, then the syntax would be `RSOR.exe <MOMDBServer\SQL_INSTANCE_NAME> <TargetAgent>`. The text file so created will list the enabled and disabled rules associated with that agent.

Export Rules Associated to an Agent Script

You can download a free script from Huntland Services to export the MOM rules that are associated with an agent from www.huntland.co.uk/Downloads/MOM/DumpMomRulesForComputerCMD.html.

The script will export the enabled rules for an agent into a CSV (comma-separated value) file.

Checking When Changes Were Made to Rules and Scripts

At times, it is handy to check when, where, and by whom changes were made to the rules. You can run the following SQL statements against the OnePoint database.

Example 1: This statement will list all rules and show when they were modified and by whom:

```
select idprocessrule, name, lastmodified, lastmodifiedby,
IsRuleGroup from OnePoint..processrule
```

Example 2: This statement will list a rule identified by its rule GUID:

```
select idprocessrule, name, lastmodified, lastmodifiedby,
IsRuleGroup from OnePoint..processrule where
idprocessrule = 'enter guid here'
```

For example

```
select idprocessrule, name, lastmodified, lastmodifiedby,
IsRuleGroup from OnePoint..processrule
where idprocessrule = '6C85049A-5F96-48DD-891F-046F3FBEF20F'
```

Example 3: This statement displays a list of scripts sorted by last modified date:

```
select name, isdeleted, lastmodified, lastmodifiedby, timeadded,
description from script
order by lastmodified desc
```

Example 4: This statement lists modification details of global settings:

```
select datacategory + dataname as GlobalSetting, datavalue,
lastmodified, lastmodifiedby from OnePoint..configuration
where lastmodifiedby != 'NULL'
```

Third-Party Tools

Numerous third-party vendors have released management packs and tools to manage MOM. The advantages of some of these management packs are that they fill in the gaps in which Microsoft or other vendors have not released a management pack, or extend MOM to monitor non-Windows systems (e.g., UNIX).

These management packs incur a cost, but they can provide a ready-made monitoring solution so that you don't have to develop your own management pack. You can find a list of the main third-party management packs in the Management Pack and Utilities catalog, available on the Microsoft web site at www.microsoft.com/management/mma/catalog.aspx.

Note Not too many third-party tools assist in managing the management pack life cycle. Currently, only Silect Software has products available to help you in this area. You can find more information at www.silect.com/products/products_overview.htm.

Summary

This chapter has explained how to manage the management pack life cycle; this will help to reduce the complexity of managing your MOM environment. The management pack life cycle can be one of the biggest headaches for a MOM administrator, so it is important that you use the information in this chapter to help you define a process that your organization will follow. The chapter has also shown how to extend MOM to monitor SNMP-enabled devices and what management packs you should install to monitor the key components of your infrastructure. Chapter 4 will cover the process you need to follow to ensure that your MOM infrastructure remains healthy.