SYNGRESS®

4 FREE BOOKLETS
YOUR SOLUTIONS MEMBERSHIP

How to Cheat at Managing Microsoft Operations Manager 2005

In the Land of the Blind, the One-Eyed Man Is King

- The Perfect Guide if "System Administrator" Is NOT Your Primary Job Function
- Avoid Time Drains Associated with Implementing MOM 2005
- Efficiently Monitor Critical Microsoft Packages such as Active Directory, Exchange, and SQL

Tony Piltzecker Technical Editor
Brian Barber • Michael Cross • Rogier Dittner
Rory McCaw • Gordon McKenna
Paul Summitt • David Williams

FOREWORD BY
DR. THOMAS W. SHINDER
CO-OWNER OF TACTEAM

Register for Free Membership to

solutions@syngress.com

Over the last few years, Syngress has published many best-selling and critically acclaimed books, including Tom Shinder's *Configuring ISA Server 2004*, Brian Caswell and Jay Beale's *Snort 2.1 Intrusion Detection*, and Angela Orebaugh and Gilbert Ramirez's *Ethereal Packet Sniffing*. One of the reasons for the success of these books has been our unique **solutions@syngress.com** program. Through this site, we've been able to provide readers a real time extension to the printed book.

As a registered owner of this book, you will qualify for free access to our members-only solutions@syngress.com program. Once you have registered, you will enjoy several benefits, including:

- Four downloadable e-booklets on topics related to the book. Each booklet is approximately 20-30 pages in Adobe PDF format. They have been selected by our editors from other best-selling Syngress books as providing topic coverage that is directly related to the coverage in this book.
- A comprehensive FAQ page that consolidates all of the key points of this book into an easy-to-search web page, providing you with the concise, easy-to-access data you need to perform your job.
- A "From the Author" Forum that allows the authors of this book to post timely updates and links to related sites, or additional topic coverage that may have been requested by readers.

Just visit us at **www.syngress.com/solutions** and follow the simple registration process. You will need to have this book with you when you register.

Thank you for giving us the opportunity to serve your needs. And be sure to let us know if there is anything else we can do to make your job easier.

SYNGRESS®

SYNGRESS®

How to Cheat at Managing Microsoft Operations Manager 2005

Tony Piltzecker Technical Editor
Brian Barber
Michael Cross
Rogier Dittner
Rory McCaw
Gordon McKenna
Paul Summitt
David Williams

FOREWORD BY
DR. THOMAS W. SHINDER

Syngress Publishing, Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively "Makers") of this book ("the Work") do not guarantee or warrant the results to be obtained from the Work.

There is no guarantee of any kind, expressed or implied, regarding the Work or its contents. The Work is sold AS IS and WITHOUT WARRANTY. You may have other legal rights, which vary from state to state.

In no event will Makers be liable to you for damages, including any loss of profits, lost savings, or other incidental or consequential damages arising out from the Work or its contents. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

You should always use reasonable care, including backup and other appropriate precautions, when working with computers, networks, data, and files.

Syngress Media®, Syngress®, "Career Advancement Through Skill Enhancement®," "Ask the Author UPDATE®," and "Hack Proofing®," are registered trademarks of Syngress Publishing, Inc. "Syngress: The Definition of a Serious Security Library"™, "Mission Critical™," and "The Only Way to Stop a Hacker is to Think Like One™" are trademarks of Syngress Publishing, Inc. Brands and product names mentioned in this book are trademarks or service marks of their respective companies.

KEY	SERIAL NUMBER
001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	HPE4F6VC87
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY
Syngress Publishing, Inc.
800 Hingham Street
Rockland, MA 02370

How to Cheat at Managing Microsoft Operations Manager 2005
Copyright © 2006 by Syngress Publishing, Inc. All rights reserved. Printed in Canada. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Printed in Canada
1 2 3 4 5 6 7 8 9 0
ISBN: 1597492515

Publisher: Andrew Williams
Acquisitions Editor: Gary Byrne
Technical Editor: Tony Piltzecker
Cover Designer: Michael Kavish
Page Layout and Art: Patricia Lupien
Copy Editor: Adrienne Rebello, Mike McGee
Indexer: Odessa&Cie

Distributed by O'Reilly Media, Inc. in the United States and Canada.
For information on rights, translations, and bulk sales, contact Matt Pedersen, Director of Sales and Rights, at Syngress Publishing; email matt@syngress.com or fax to 781-681-3585.

Acknowledgments

Syngress would like to acknowledge the following people for their kindness and support in making this book possible.

Syngress books are now distributed in the United States and Canada by O'Reilly Media, Inc. The enthusiasm and work ethic at O'Reilly are incredible, and we would like to thank everyone there for their time and efforts to bring Syngress books to market: Tim O'Reilly, Laura Baldwin, Mark Brokering, Mike Leonard, Donna Selenko, Bonnie Sheehan, Cindy Davis, Grant Kikkert, Opol Matsutaro, Steve Hazelwood, Mark Wilson, Rick Brown, Tim Hinton, Kyle Hart, Sara Winge, C. J. Rayhill, Peter Pardo, Leslie Crandell, Regina Aggio, Pascal Honscher, Preston Paull, Susan Thompson, Bruce Stewart, Laura Schmier, Sue Willing, Mark Jacobsen, Betsy Waliszewski, Kathryn Barrett, John Chodacki, Rob Bullington, Aileen Berg, and Wendy Patterson.

The incredibly hardworking team at Elsevier Science, including Jonathan Bunkell, Ian Seager, Duncan Enright, David Burton, Rosanna Ramacciotti, Robert Fairbrother, Miguel Sanchez, Klaus Beran, Emma Wyatt, Chris Hossack, Krista Leppiko, Marcel Koppes, Judy Chappell, Radek Janousek, and Chris Reinders for making certain that our vision remains worldwide in scope.

David Buckland, Marie Chieng, Lucy Chong, Leslie Lim, Audrey Gan, Pang Ai Hua, Joseph Chan, and Siti Zuraidah Ahmad of STP Distributors for the enthusiasm with which they receive our books.

David Scott, Tricia Wilden, Marilla Burgess, Annette Scott, Andrew Swaffer, Stephen O'Donoghue, Bec Lowe, Mark Langley, and Anyo Geddes of Woodslane for distributing our books throughout Australia, New Zealand, Papua New Guinea, Fiji, Tonga, Solomon Islands, and the Cook Islands.

Lead Author and Technical Editor

Tony Piltzecker (CISSP, MCSE, CCNA, CCVP, Check Point CCSA, Citrix CCA), author and technical editor of Syngress Publishing's *MCSE Exam 70-296 Study Guide and DVD Training System,* is a Consulting Engineer for Networked Information Systems in Woburn, MA.

Tony's specialties include network security design, Microsoft operating system and applications architecture, as well as Cisco IP Telephony implementations. Tony's background includes positions as IT Manager for SynQor Inc., Network Architect for Planning Systems, Inc., and Senior Networking Consultant with Integrated Information Systems. Along with his various certifications, Tony holds a bachelor's degree in business administration. Tony currently resides in Leominster, MA, with his wife, Melanie, and his daughters, Kaitlyn and Noelle.

Technical Reviewer

Brian Barber (MCSE, MCP+I, MCNE, CNE-5, CNE-4, CNA-3, CNA-GW) is coauthor of Syngress Publishing's *Configuring Exchange 2000 Server* (ISBN: 1-928994-25-3), *Configuring and Troubleshooting Windows XP Professional* (ISBN: 1-928994-80-6), and two study guides for the MSCE on Windows Server 2003 track (exams 70-296 [ISBN: 1-932266-57-7] and 70-297 [ISBN: 1-932266-54-2]). He is a Senior Technology Consultant with Sierra Systems Consultants Inc. in Ottawa, Canada. He specializes in IT service management and technical and infrastructure architecture, focusing on systems management, multiplatform integration, directory services, and messaging. In the past he has held the positions of Senior Technical Analyst at MetLife Canada and Senior Technical

Coordinator at the LGS Group Inc. (now a part of IBM Global Services).

Brian also contributed to the technical editing of this book.

Contributing Authors

Michael Cross (MCSE, MCP+I, CNA, Network+) is an Internet Specialist/Computer Forensic Analyst with the Niagara Regional Police Service (NRPS). He performs computer forensic examinations on computers involved in criminal investigation. He also has consulted and assisted in cases dealing with computer-related/Internet crimes. In addition to designing and maintaining the NRPS Web site at www.nrps.com and the NRPS intranet, he has provided support in the areas of programming, hardware, and network administration. As part of an information technology team that provides support to a user base of more than 800 civilian and uniform users, he has a theory that when the users carry guns, you tend to be more motivated in solving their problems.

Michael also owns KnightWare (www.knightware.ca), which provides computer-related services such as Web page design, and Bookworms (www.bookworms.ca), where you can purchase collectibles and other interesting items online. He has been a freelance writer for several years, and he has been published more than three dozen times in numerous books and anthologies. He currently resides in St. Catharines, Ontario, Canada, with his lovely wife, Jennifer, his darling daughter, Sara, and charming son, Jason.

Rogier Dittner (MCSE NT4, 2000, 2003, MCDBA, MCT, MFS Practitioner) is a consultant with a gold certified Microsoft partner offering solutions based on Microsoft technology to customers. As a consultant he supports the sales organization and takes part in planning and designing complex Microsoft-oriented implementations.

Because of his personal interests and more than 10 years' experience, he has deep technical working knowledge in a broad range of Microsoft products. Within his company he performs the leading role in operations management solutions and training.

He would like to thank his wife and children for giving him the time and space to write (Pascalle, bedankt, je bent een schat!).

Rory McCaw (MCSE, MCP+!, and MCT) is a Senior Technical Consultant, Trainer, accomplished presenter, and author of numerous published technical books. He has more than 10 years of experience in the information technology industry.

Rory's focus is on operations management and security. He helps organizations to implement security standards to comply with government and SEC regulations, such as SOX, as well as effectively monitor their server infrastructures. Rory has developed and delivered presentations for Microsoft at COMDEX, the Worldwide Partner Conference, and worldwide Train the Trainer events. Rory is also actively involved in the design of custom courses and hands-on labs used at various Microsoft workshops and seminars. He holds a bachelor's degree in administration from Lakehead University.

Gordon McKenna (MCSE) is an Independent Technical Consultant and one of the U.K.'s leading MOM specialists. He has more than six years' experience in the technology from his early days as a management specialist with Mission Critical Software and NetIQ.

Gordon has a host of successful, large-scale MOM deployments to his credit and is one of the leading evangelists for the technology. He regularly presents at events and actively supports the growing MOM community.

Paul Summitt (MCSE, CCNA, MCP+I, MCP) holds a master's degree in mass communication. Paul has served as a network, an Exchange, and a database administrator, as well as a Web and appli-

cation developer. Paul has written on virtual reality and Web development and has served as technical editor for several books on Microsoft technologies. Paul lives in Columbia, MO, with his life and writing partner, Mary.

David Williams works as an Infrastructure Manager for the John H. Harland Company in Atlanta, GA. Harland is one of the leading software companies focused on financial institutions, one of the largest check printers in the country, and the leader in testing and assessment solutions for the education market. In addition to managing IT resources, he is also a senior architect and an advisory engineer, providing technical direction and advice to Harland's management team in long-range planning for new or projected areas of enterprise projects.

He is also a principal at Williams & Garcia, LLC, a consulting practice specializing in delivering effective enterprise infrastructure solutions. He specializes in the development of advanced solutions based on Microsoft technologies and strategic infrastructure designs.

David studied Music Engineering Technology at the University of Miami, and he holds MCSE, MCDBA, VCP, and CCNA certifications.

When not rearchitecting corporate infrastructures, he spends his time with his wife and three children.

Foreword Contributor

Thomas W. Shinder, MD, (MCSE), has been awarded the Microsoft Most Valuable Professional (MVP) award for his work with ISA Server and is recognized in the firewall community as one of the foremost experts on ISA Server. Tom has consulted with major companies and organizations such as Microsoft Corp., Xerox, Lucent Technologies, FINA Oil, Hewlett-Packard, and the U.S. Department of Energy.

Tom practiced medicine in Oregon, Texas, and Arkansas before turning his growing fascination with computer technology into a new career shortly after marrying his wife, Debra Littlejohn Shinder, in the mid 1990s. They co-own TACteam (Trainers, Authors, and Consultants), through which they teach technology topics and develop courseware; write books, articles, white papers, and corporate product documentation and marketing materials; and assist small and large businesses in deploying technology solutions.

Tom coauthored, with Deb, the best-selling *Configuring ISA Server 2000* (Syngress Publishing, ISBN: 1-928994-29-6), *Dr. Tom Shinder's ISA Server and Beyond* (Syngress, ISBN: 1-931836-66-3), *Troubleshooting Windows 2000 TCP/IP* (Syngress, ISBN: 1-928994-11-3), and *Dr. Tom Shinder's Configuring ISA Server 2004* (Syngress, ISBN: 1-931836-19-1). He has contributed to several other books on subjects such as the Windows 2000 and Windows 2003 MCSE exams and has written hundreds of articles on Windows server products for a variety of electronic and print publications.

Tom is the "primary perpetrator" on ISAserver.org (www.isaserver.org), where he answers hundreds of questions per week on the discussion boards and is the leading content contributor.

Contents

Foreword

When you are facing a new management environment, resources such as this book are essential to your success. Here you will find all the information you need to understand how Microsoft Operations Manager (MOM) works, as well as the tools MOM provides for managing and monitoring your Windows network and servers running on that network. You need a combination of experience and knowledge to get a job done right; this book provides the knowledge you need. Rather than searching through countless CDs, DVDs, and online documentation, you can look to this book to find basic and advanced concepts, such as MOM 2005 essentials, troubleshooting MOM, and understanding and deploying management packs, as well as helpful tips and tricks to get the most out of MOM.

Our success as network managers is often judged by our ability to find and fix server and network-based problems quickly. In the past, the process was often a hit-or-miss proposition, worsened by difficult-to-use vendor documentation. I have spent countless hours, both online and in person, helping hapless network administrators get a handle on problems that they could not solve because of inadequate documentation. For users of MOM, however, this will not be an issue; I can refer all MOM administrators to this book to get all the information they need.

—Dr. Thomas W. Shinder
Co-owner TACteam

About the Book

How to Cheat at Managing Microsoft Operations Manager 2005 is written for system administrators and systems engineers who are responsible for the upkeep and administration of IT environments, from a two server environment to a large enterprise. This book will is a must-read for anyone looking at implementing an enterprise management solution, and is specifically interested in the Microsoft Operations Manager 2005 offering.

Ten Benefits of Reading This Book

- Understand the ideal setting for an implementation of Microsoft Operations Manager 2005.
- Determine which MOM product is right for your environment.
- Formulate a strategic plan for implementing MOM 2005.
- Follow step-by-step instructions for implementing MOM 2005.
- Discover in-depth knowledge of key MOM Management Packs.
- Learn how to manage and monitor non-Microsoft platforms.
- Learn how to monitor critical Microsoft packages such as Active Directory, Exchange, and SQL.
- Receive troubleshooting techniques for common MOM issues.
- Provides an overview of the Microsoft Systems Center initiative.
- A great shelf-reference for any MOM administrator.

Chapter 1

Microsoft Operations Manager 2005 Essentials

Solutions in this chapter:

- **Introducing Microsoft Operations Manager**
- **Features of Microsoft Operations Manager**
- **Microsoft MOM Workgroup Edition**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

You may be hearing about Microsoft MOM for the first time, or maybe you've been using it for a number of years. In either case, it is always best to start from scratch and begin the coverage of MOM with the basics. Even if you're a MOM expert, there may be things you don't know (or have forgotten). The goal of this chapter is to cover the basics of MOM, introduce you to the concept of centralized management, outline the features of MOM, and break down the various versions available to you.

Introducing Microsoft Operations Manager

Microsoft Operations Manager (MOM) 2005 is one of those products that has "flown under the radar" for a number of years. With enterprise IT shops getting larger by the day, the ability to centralize management for ease of administration has become more in demand as of late. As a result, MOM and its counterparts from other vendors are rising in prominence.

MOM is Microsoft's latest effort to assist IT professionals in their quest to ease the administrative burden they must face. Microsoft MOM, originally introduced in 2000, is intended to provide proactive support to impending IT issues, as opposed to the normal "fire-fighting" that most IT shops are forced into after a problem has already occurred. Microsoft has positioned MOM to address several operational issues:

- Event Management
- Proactive Alerting
- Reporting
- Trend Analysis

MOM is intended to help IT professionals reduce the amount of time spent on IT issue discovery and troubleshooting by putting a wide variety of management tools (called management packs) into a single, user-friendly interface. By centralizing management and monitoring into a single console, MOM's goal is to reduce the amount of reactive responses to issues, determine the root cause of a problem, and provide possible solutions to many known issues.

MOM not only deals with issues as they occur but also helps your overall Operations functions through the use of Solutions Accelerators. Solutions

Accelerators are best practice solutions provided by Microsoft to address a number of common Operations goals. Microsoft is so committed to the idea of Solutions Accelerators within MOM that it is a part of the larger Microsoft Operations Framework (for more information on the MOF, visit http://www.microsoft.com/technet/itsolutions/cits/mo/mof/mofeo.mspx). Currently, there are five Solutions Accelerators:

- **Notification Workflow Solution Accelerator** Extends notification functions inside of MOM, providing the ability for selective alerting based on preset criteria.
- **Autoticketing Solutions Accelerator** Provides for automatic creation of trouble tickets in the Trouble Ticket system.
- **Alert Tuning Solutions Accelerator** Helps to limit the amount of unnecessary alerts while installing a management pack.
- **Service Continuity Solutions Accelerator** Helps to maintain high availability of MOM services.
- **Multiple Management Group Rollup Solutions Accelerator** Allows for consolidation of multiple management groups into a single, centralized solution.

The Multiple Management Group Rollup Solutions Accelerator is a great lead-in for a discussion of the concept of centralized operations management.

Understating Centralized Operations Management

Centralized management as a whole has been a goal of many organizations for a number of years. The ability to reduce overhead, streamline and consolidate technologies, and minimize complexity is a never-ending process. Take for example the concept behind Active Directory (AD). The goal of AD was to reduce the number of NT domains, domain trusts, administrators, and so on. We took potentially hundreds of domains and rolled them into a single domain (or two domains if you use the trusted root model) and Organizational Units (OU) (see Figures 1.1 and 1.2).

Figure 1.1 Converting Multiple NT Domains into a Single Active Directory Domain

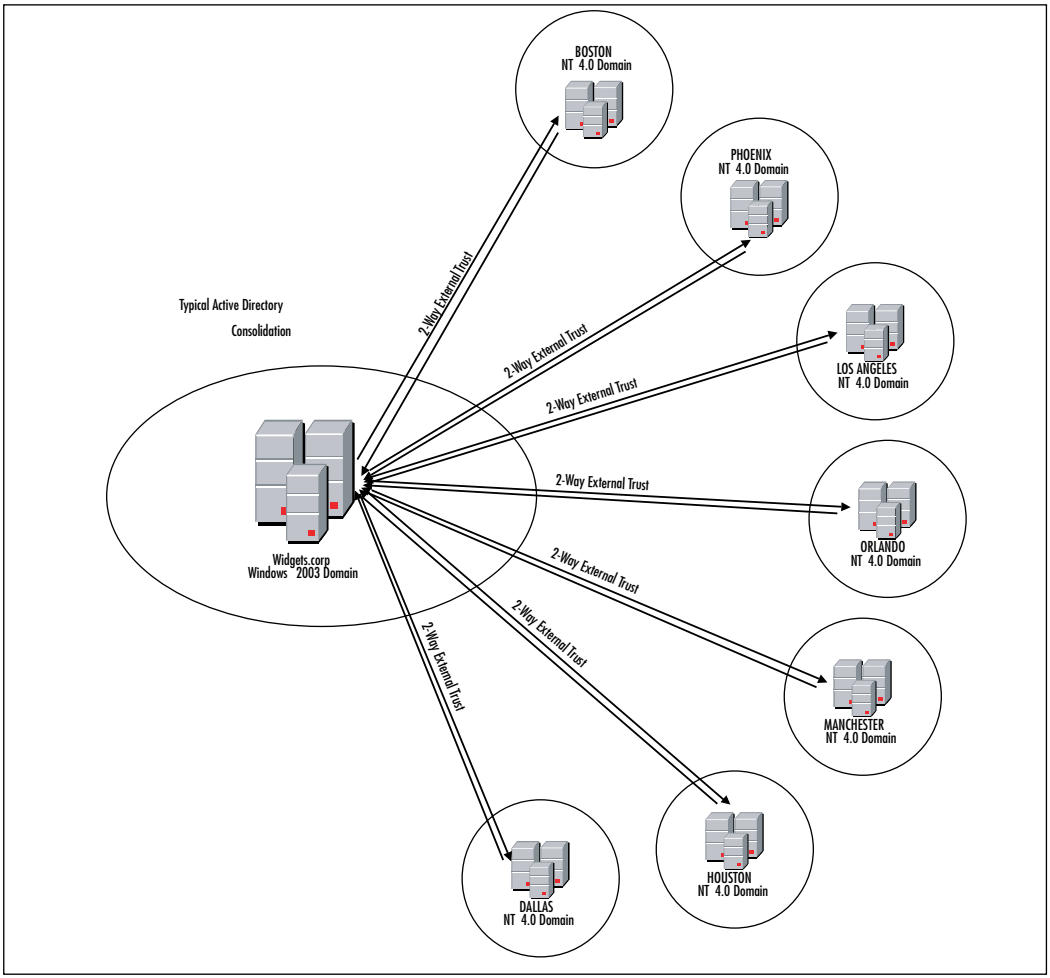
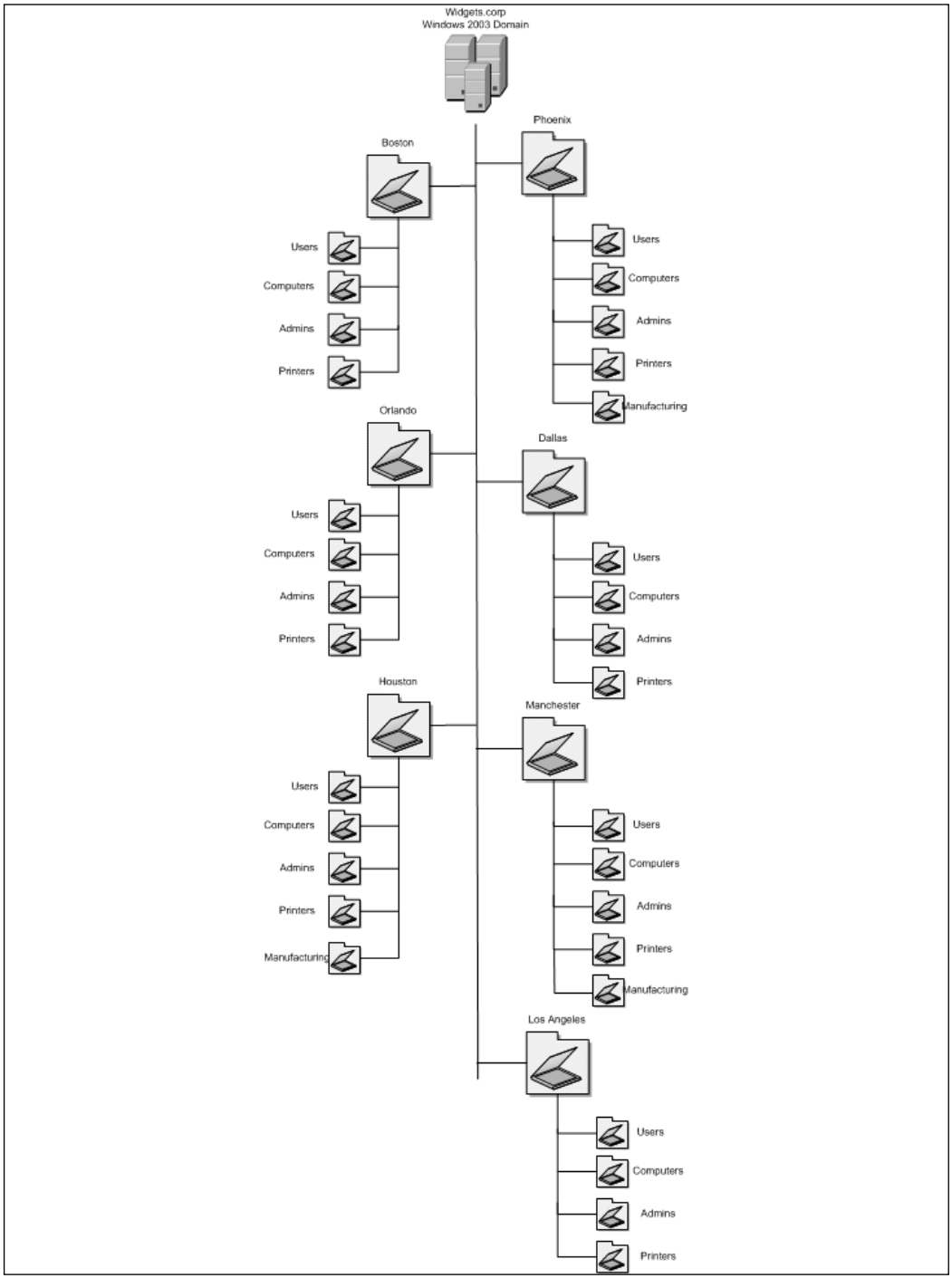


Figure 1.2 Domains Consolidated into OUs



By consolidating AD, we found that we were able to reduce the amount of potential issues caused by crossing multiple domains due to trusts, nested group permissions, and so forth. On a different spin, the concept of a Network Operations Center (NOC) has been around for many years as well. However, for midsized companies, having a guy sitting in a big room in front of dozens of monitors, playing "the man behind the curtain" isn't a realistic scenario. In a NOC environment, there is typically 24/7 support for these systems, where regular hardware and application checkups can be performed. In the midsized environment, the IT administrator or engineer may be able to perform system checks only on an infrequent basis due to his or her daily responsibilities.

Many software development companies have tried to address this issue, as well as some hardware companies. For example, there are very basic monitoring packages such as Ipswitch WhatsUp Gold, and there are some very robust packages, such as HP OpenView. With the basic packages, they typically missed the boat on many levels, but were good enough to let you know if a system crashed or a service stopped. Packages like HP OpenView usually required someone with extensive OpenView experience, which meant you had to hire someone to monitor your HP OpenView.

As time progressed, packages that were more middle-of-the-road began to appear. For example, NetIQ released its AppManager suite of products. Finally! A package that was simple enough to manage without hiring a guru, but robust enough to get us the details we need. However, AppManager was still lacking in many areas, since it was still unable to manage several applications and hardware platforms.

When MOM was introduced in the year 2000, the idea was simple: provide a single-point solution for managing many of Microsoft's packages. Unfortunately, with the introduction of Active Directory in the same year (as well as the infamous Y2K), MOM didn't get the respect it should have received. It did exactly what it was intended to do, but as with many products, it had its issues. Specifically, MOM 2000 was often considered to be too rough bulky from a client rollout and management perspective. Typically, network latency was a huge issue across large networks, the size of the MOM agents were large (22 megabytes), and these problems could be seen when monitoring a system via MOM 2000.

That brings us Microsoft MOM 2005. Microsoft MOM 2005 was released to the market in late 2004/early 2005; Microsoft had addressed many of these issues. Network discovery was reduced to one-fifth of that in 2000, latency was greatly reduced, and the agents were reduced to only 3.5MB! Finally, a product that we could use without pulling our hair out! Certainly, improving network performance and shrinking the size of the client agent can't be the improvements. Let's move ahead now and talk about what else is new in MOM 2005.

What's New in MOM 2005?

In the previous section, we discussed how Microsoft had made improvements to MOM over the previous version. Along with these improvements, Microsoft made several additional improvements to MOM 2005:

- **Better Reporting** Over 100 canned reports, ability to easily create custom reports, improved data mining.
- **More Management Packs** Following Microsoft's Common Engineering Roadmap, all Microsoft products will now have a associated management packs. Microsoft has also made it a goal to develop monitoring functions right into the applications!
- **Improved User Interface** Microsoft has introduced new views into the user interface.

Along with the aforementioned items, Microsoft has worked diligently to add additional functionality into MOM 2005 above and beyond that of MOM 2000. Let's take a look at some of those features, as well as an overall description of all the MOM 2005 features.

Features of Microsoft Operations Manager

We've now talked a little bit about some of features and benefits of Microsoft Operations Manager 2005, but we still need to discuss exactly what goes into the MOM 2005 product. There are many components that make up the MOM 2005 product, but there are five specific areas that Microsoft outlines as the key components of MOM. Let's discuss the five main areas of the MOM 2005 product.

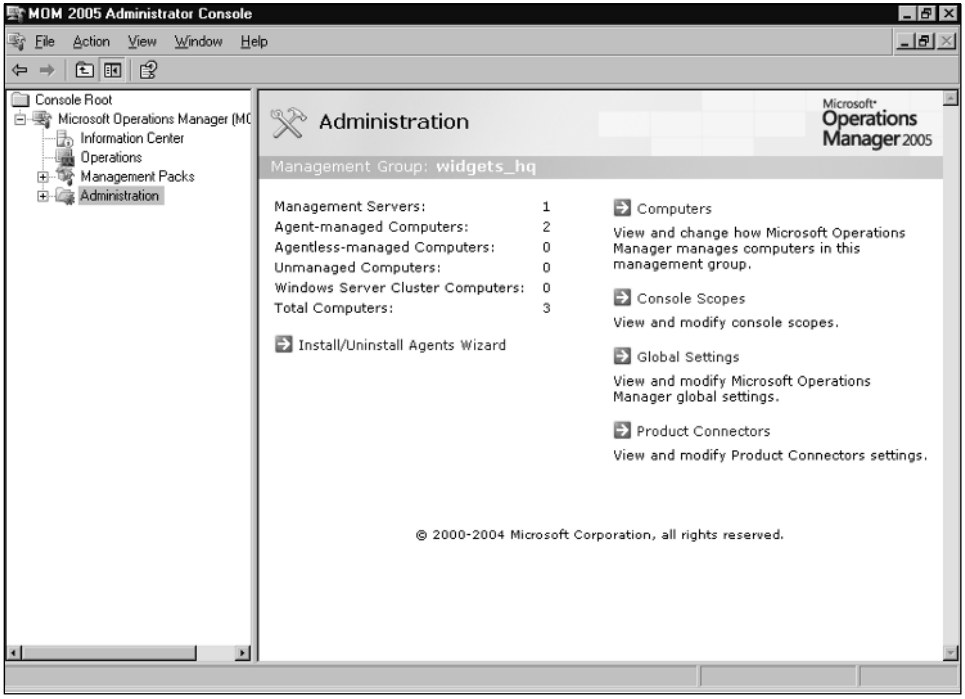
User Interfaces

The Microsoft MOM user interfaces are divided into four main consoles: Administrator, Operations, Reporting, and Web. Each console serves a different purpose in using Microsoft MOM 2005.

Administrator Console

In this console, you can perform a variety of functions including system discovery, agent deployment, and management pack administration (see Figure 1.3).

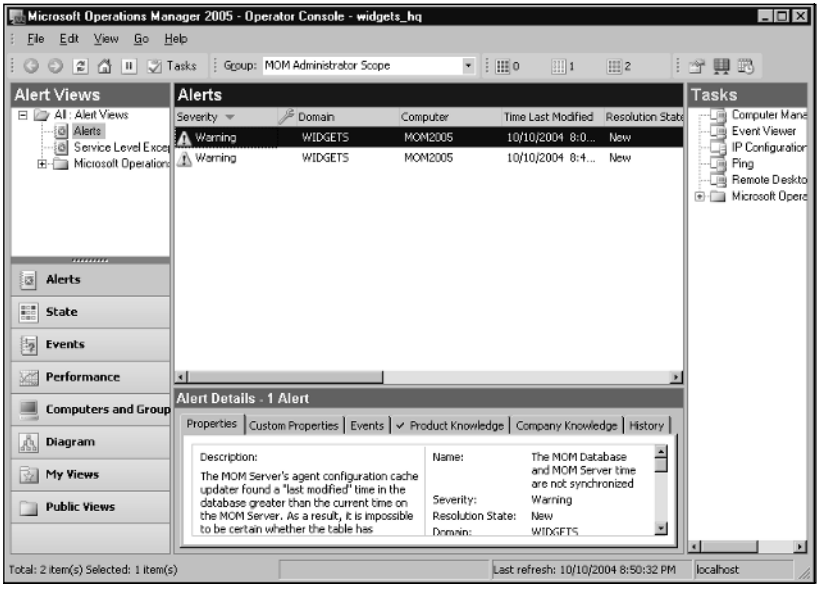
Figure 1.3 Administrator Console



Operations Console

This console is the main window for MOM 2005. In this console, you can monitor the health of your systems, as well as recommended solutions for any existing issues. This console is customizable for enterprise-specific troubleshooting data (see Figure 1.4).

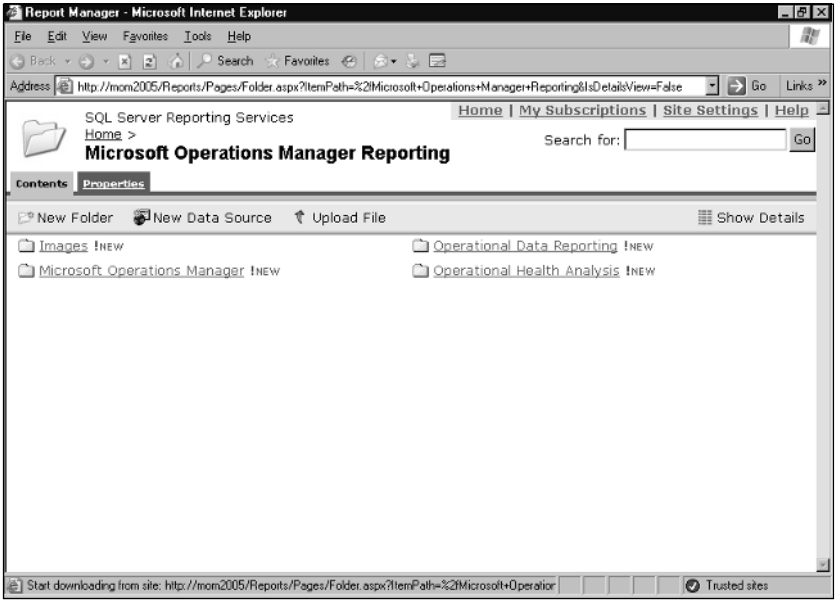
Figure 1.4 Operations Console



Reporting Console

This console is used to view Microsoft MOM-specific reports from within a Web browser (see Figure 1.5).

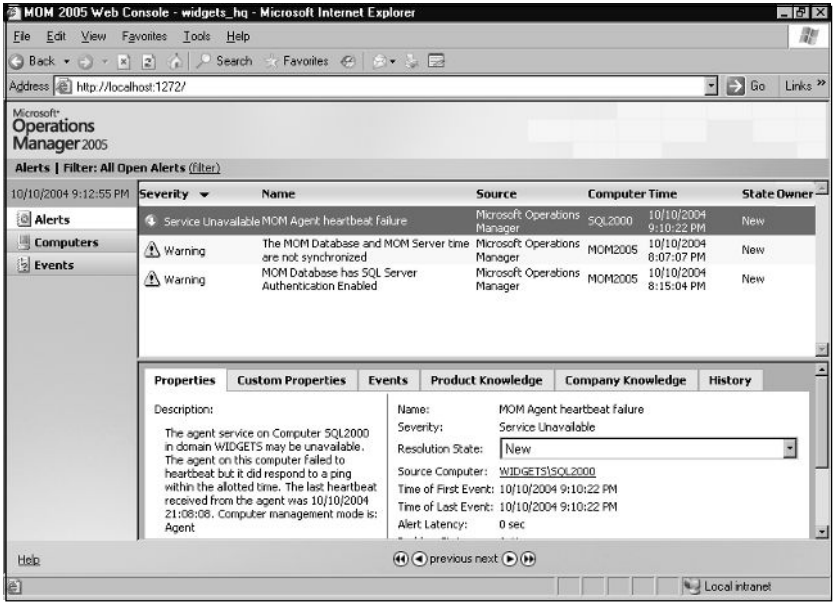
Figure 1.5 Reporting Console



Web Console

As with the Reporting console, the Web console allows for an administrator to monitor his or her system from a Web browser, allowing for remote monitoring without using the full client (see Figure 1.6).

Figure 1.6 Web Console



Operations

Microsoft MOM 2005 Operations are the functions that can be performed within the MOM 2005 platform. These are the "bells and whistles" of MOM 2005 that allow you to customize your MOM experience to best suit your IT operational needs. Table 1.1 outlines some of the different operational functions and features in MOM 2005.

Table 1.1 MOM Operations Features

Feature	Description
Auto-Alert Resolution	Allows MOM to update its database when a problem has been corrected without user intervention.
Cluster-Aware Monitoring	Microsoft MOM can be configured to discover cluster server configurations and monitor both the physical and virtual servers.
Instance-Aware Monitoring	MOM can look inside of a SQL server and monitor not only SQL as a whole, but also individual SQL database instances.
Maintenance Mode	Allows you to put a server in a maintenance state to prevent alerts while system maintenance is occurring.

Security

Microsoft has designated security as a key strategic initiative in all its products. It only makes sense, therefore, that security would be a key feature in any management and monitoring product that Microsoft would release into the marketplace. Some of the security features involve the underlying MOM services; others are more operator-specific. Table 1.2 outlines three of the security features.

Table 1.2 MOM Security Features

Feature	Description
Secure Communications	To prevent a would-be hacker from gaining information about your network owing to unsecured transmission of MOM monitoring alerts and updates, Microsoft has secured the communications between the remote agents and the MOM server.
Delegation of Authority	Much like delegation in Active Directory or Exchange, MOM has been built to allow administrators to set different user security levels for a variety of items.
Secured Services	MOM no longer needs to run on a Local System account, but rather on a Network Service account, thus providing an additional layer of security to the MOM platform.

Deployment

This is where things get really interesting. In small environments, walking over to rack of servers and installing an agent is a piece of cake. What if you have a distributed network with data centers in offices across town, across the country, or across the world? What if you are running on multiple hardware platforms? Don't worry; MOM has thought of everything (and she even packed you a nice lunch!). Table 1.3 outlines some of the deployment advantages of MOM 2005.

Table 1.3 MOM Deployment Features

Feature	Description
64-bit Support	Allows MOM to manage the 64-bit version of Windows 2003 and applications running on it.
Agentless Monitoring	In certain scenarios, you may not be able to load an agent onto a system. MOM can manage a limited number of servers without loading an agent (with certain limitations).
Internationalization	If you have servers in various parts of the world, MOM can adjust for locales and languages.
Server Discovery	MOM provides a great wizard for importing server data from sources such as Active Directory.

Some Independent Advice

The 64-bit support is huge! With the rapid drop in price of 64-bit processors and the introduction of SQL 2005 on 64-bit, supporting this platform is going to be crucial to your environment. As more and more applications are developed for 64-bit processing, you will begin to understand just how important this feature will become!

Reporting

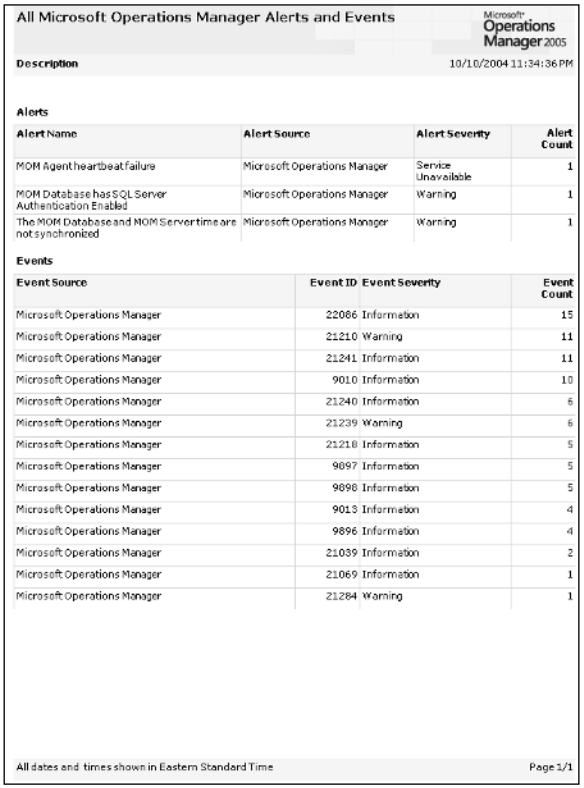
As important as it is to be able to manage, monitor, and collect data about your environment, it is equally as important to be able to report on that data. As the saying goes, a picture is worth a thousand words. It's one thing to be able to tell management that there's a problem with the environment, it's another to be able to

create crisp, formatted reports to show exactly where the problem exists. We mentioned earlier how Microsoft had improved reporting by integrating it with SQL Server, but it is also noteworthy to point out the varies types of formats MOM can export the reports to:

- Microsoft Excel
- Adobe Acrobat (PDF)
- HTML
- Graphic files (TIFF)
- Comma-delimited files (CSV)
- XML

By providing the ability to export to multiple data formats, MOM has made your job easier when it comes to justifying cost to upper management. Figure 1.7 shows a sample .tif file format report.

Figure 1.7 .Tif-Formatted MOM Report



All Microsoft Operations Manager Alerts and Events

Microsoft Operations Manager 2005

Description 10/10/2004 11:34:36 PM

Alerts

Alert Name	Alert Source	Alert Severity	Alert Count
MOM Agent heartbeat failure	Microsoft Operations Manager	Service Unavailable	1
MOM Database has SQL Server Authentication Enabled	Microsoft Operations Manager	Warning	1
The MOM Database and MOM Server time are not synchronized	Microsoft Operations Manager	Warning	1

Events

Event Source	Event ID	Event Severity	Event Count
Microsoft Operations Manager	22086	Information	15
Microsoft Operations Manager	21210	Warning	11
Microsoft Operations Manager	21241	Information	11
Microsoft Operations Manager	9010	Information	10
Microsoft Operations Manager	21240	Information	6
Microsoft Operations Manager	21239	Warning	6
Microsoft Operations Manager	21218	Information	5
Microsoft Operations Manager	9097	Information	5
Microsoft Operations Manager	9098	Information	5
Microsoft Operations Manager	9013	Information	4
Microsoft Operations Manager	9896	Information	4
Microsoft Operations Manager	21039	Information	2
Microsoft Operations Manager	21069	Information	1
Microsoft Operations Manager	21284	Warning	1

All dates and times shown in Eastern Standard Time Page 1/1

Some Independent Advice

Reporting is one area where you can really "think outside the box." Depending on your scripting skills, you can get pretty creative with these reports. If you have HTML enabled in your e-mail client, you can be proactive in scheduling reports to print and e-mail to a distribution group on a daily basis!

Discussing reporting and its importance to the MOM 2005 solution is probably a good place to transition into a conversation about "MOM lite," otherwise known as MOM 2005 Workgroup Edition.

Microsoft MOM 2005 Workgroup Edition

Reporting gives you a good segue into a conversation about MOM 2005 Workgroup Edition because reporting is the one thing that MOM 2005 is missing; however, it is not the only feature that separates Microsoft MOM 2005 from MOM 2005 Workgroup Edition. Let's compare the two products.

Comparing MOM 2005 with MOM 2005 Workgroup Edition

The most important thing to point out about MOM 2005 and MOM 2005 Workgroup Edition is that besides limitations on licenses and the fact that reporting is not available, MOM 2005 Workgroup Edition has the same look and feel as MOM 2005. You can still use the same management packs, you can still deploy agents, use agentless monitoring, provide Web-based administration, and so on. Along with reporting, the following items are included in the full Microsoft MOM 2005 package, but not in the Workgroup Edition:

- MOM Connector Framework
- SQL Server Reporting and Database
- Software Assurance and Licensing

Let's briefly discuss each of these one by one.

MOM Connector Framework

The MOM connector framework is intended to allow MOM 2005 users to integrate with third-party management tools such as Tivoli, NetIQ, and so on. The reason for this feature being left out of the Workgroup product is the assumption that the Workgroup Edition is being used in a small environment where large third-party packages, such as OpenView or Tivoli, will not be used. We will discuss connecting to third-party products later in Chapter 11.

SQL Server Reporting and Database

Microsoft MOM 2005 requires a fully licensed copy of SQL Server 2000 for its back-end database and reporting functionality. To keep Workgroup Edition from being too cost prohibitive, Microsoft has enabled MOM Workgroup Edition to function with the SQL Server 2000 Desktop Edition (MSDE). MSDE is a stripped-down version of the full SQL server package, and it's a free download from Microsoft! The downside to MSDE is that it cannot hold as many records as the full SQL package, and reporting is not an option.

Software Assurance and Licensing

Software Assurance is a licensing initiative brought forth to help customers keep their Microsoft licensing accurate by providing them with the ability to upgrade to the latest versions of their software "free of charge" while they are under the Software Assurance program. Unfortunately, MOM 2005 does not fall under this offering. For more information on Software Assurance, visit http://www.microsoft.com/licensing/programs/sa/default.mspx.

We also need to discuss the licensing limitations of Workgroup Edition. Specifically, it is important to note that Workgroup Edition allows for a maximum of 10 servers. If you have more than 10 servers to monitor or expect to grow rapidly in the next 18 to 24 months, then Workgroup Edition probably is not the product for you.

Some Independent Advice

Sometimes Microsoft just gets it, they really do. With MOM, Microsoft understands that the size of an IT organization will grow over time. To allow for growth, Microsoft has a very simple migration strategy to get from Workgroup edition to the full-blown MOM 2005.

Okay, now that you know the basics about MOM, its time to kick this into high-gear and start digging into the real meat of MOM!

Summary

Centralizing management has been a goal of IT professionals for years. In many ways, it has become the "Holy Grail" of IT. Everyone is looking for a way to do things faster, smarter, and easier than before. Microsoft Operations Manager 2005 is another tool in the tool belt to help IT professionals in that quest for the Holy Grail. Let's recap some of the items we've discussed:

- Microsoft Operations Manager is intended to serve as a single-product solution for managing an IT enterprise.
- Microsoft MOM 2005 has several improvements over MOM 2000, the most notable being the size of agents, and the reduction in network latency, and the introduction of agentless monitoring.
- Microsoft MOM Workgroup Edition, though still just as useful as full-blown MOM, has its limitations.
- Microsoft MOM 2005 provides for many different flavors and ways to generate reports based on collected data.

Although there are many different packages available on the market today to help you with management and monitoring of your IT enterprise, we think you will find that MOM 2005 is right up there at the top of the list because of all the bells and whistles that Microsoft has put into their offering. In an environment that is primarily Microsoft-based (Windows, Exchange, IIS, SQL, etc.), having a management package written by the vendor of these other back-office applications makes it even that more enticing. We hope that by reading the coming chapters of this book, you will have a better understanding of the product, and have the necessary tools at your fingertips to go out into the world and begin deploying MOM 2005.

Solutions Fast Track

Introducing Microsoft Operations Manager

- ☑ There are many applications available for monitoring servers.
- ☑ Microsoft MOM 2000 was introduced to monitor and manage various Microsoft products.
- ☑ MOM 2005 introduced the concept of agentless monitoring.

Features of Microsoft Operations Manager

- ☑ There are four key consoles to MOM 2005: Administrator, Operations, Reporting, and Web.
- ☑ MOM 2005 encrypts client/server traffic for security purposes.
- ☑ MOM 2005 can generate reports into several formats including CSV, TIFF, and JPG.

Microsoft MOM 2005 Workgroup Edition

- ☑ MOM 2005 Workgroup Edition can monitor up to 10 servers.
- ☑ MOM 2005 Workshop Edition can run on MSDE.
- ☑ MOM 2005 can be upgraded to full-blown MOM 2005.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: I've heard that Microsoft Operations Manager is expensive. Is that true?

A: Yes and no. There is a cost to implementing MOM, like any other product. You have to purchase a license for a MOM server, SQL, and any managed servers. However, Microsoft has many packages available for this in order to reduce costs. The good news is that all Microsoft-developed management packs are free of charge.

Q: I've heard that MOM is difficult to install and configure. Is that true?

A: You may have some trouble the first time through. This book is intended to assist you with that process, and to fill in some of the areas where confusion typically might occur.

Q: Can MOM 2005 Workgroup Edition still monitor Exchange and SQL?

A: Yes, Workgroup Edition can use the same management packs as the full-blown package.

Q: Is the Web Management console secure?

A: By default, no. However, it is a standard IIS Web site, so you can easily turn on SSL.

Q: Many management and monitoring packages do not limit authority by user IDs or groups. How does MOM address this?

A: Fear not. MOM 2005 has the ability for you to delegate authority to various parts of the MOM console by user or group.

Q: What if we outgrow MOM 2005 Workgroup Edition?

A: Microsoft has a roadmap for migration from Workgroup Edition to the full MOM 2005 package.

Q: Will MOM 2005 be able to monitor new packages and operating systems?

A: Yes. Microsoft continues to develop new management packs as new Microsoft software packages are deployed.

Chapter 2

Evaluating Your Environment

Solutions in this chapter:

- **Understanding Your Environment**
- **Identifying Requirements**
- **Selecting a Version of Microsoft Operations Manager**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

Truly understanding the environment you are about to monitor with Microsoft Operations Manager 2005 is essential to any successful planning strategy you undertake. This should be done prior to deploying and configuring the solution. Not only collecting the right information with regards to the true requirements of your organization but choosing the right version of the product to meet your needs can be the difference between success and failure of your project in the long term. In this chapter we will start with a look at the kind of information you should be collecting about your environment, how this information can be used to help you assess what your true monitoring requirements are, we will take a look at some of the tools and documentation available to help you collect the right data, as well as walking through how you select the right version of MOM to fit your needs. Once you have a grasp of the extent of planning that is required for your project and the information that is needed to make the right decisions, we will look at some of the tools available to assist you in the planning stage. This chapter will help prepare you for Chapter 3, which focuses on planning and deployment.

Understanding Your Environment

Understanding your environment in preparation for planning a Microsoft Operations Manager 2005 deployment is a critical exercise that you must undertake before moving forward. It is something that will take you to different parts of the organization, and will mean you spending time talking to key members of staff. The goal of evaluating your environment is to arm you with the information you need to be able to successfully plan for your installation of MOM 2005. The key to success of this stage will be in the knowledge you gain of the environment, your ability to obtain information from others, and the correct use of available tools and documentation.

Collecting Data about Your Enterprise

The first exercise in properly understanding the environment that you will deploy MOM into is to collect information regarding various aspects of the infrastructure.

In the following sections we will look at some of the key areas you should be focusing on along with some of the tools that are available to aid you in this process.

Network Topology

It is important to fully understand the network topology for the environment that you will deploy MOM into as this can have a dramatic effect on the success or failure of your implementation.

Key information that you need to assess at this stage is:

- Existing network protocols
- Network bandwidth
- Network hardware, such as routers, switches, and firewalls

You also need to understand about the existing network topology, network size, type of network, and traffic patterns, in addition to the logical organization of the network, name-resolution and address-resolution methods, naming conventions, and network services in use.

Most organizations should be able to provide you with some kind of network diagram containing at least some of this information; if these are not available you could utilize one of the Windows Server 2003 diagnostic applications, such as Network Monitor to help gather the information about your network alternatively. There are a number of third-party tools available that can make this task easier.

Once you have collected the data you need, you can create both physical and logical network diagrams using products such as Microsoft® Visio®.

The physical and logical network diagrams should include the following information:

- Physical communication links, including cables and the paths of analog and digital lines.
- Server names, IP addresses, and domain membership.
- Location of printers, hubs, switches, routers, bridges, proxy servers, and other network devices.
- Wide area network (WAN) communication links, their speed, and available bandwidth between sites. If you have slow or heavily used connections, it is important to note them.
- Physical network infrastructure.
- Addressing infrastructure.
- Naming infrastructure.
- Authentication infrastructure.

- Security infrastructure.
- Intranet infrastructure.
- Management infrastructure.

The logical network diagram should also include the following information:

- Domain architecture
- Server roles
- Trust relationships and any policy restrictions that might affect your deployment

Finally, be sure to address network security measures in your assessment of the network. Include information about how you manage client authentication, user and group access to resources, and Internet security. Also include your firewall and proxy configurations.

Figure 2.1 is an example of a typical network diagram for an organization, in a classic hub–spoke layout; this is ideal for understanding what bandwidth you have between your central components and your remote agents as each of the individual link speeds is highlighted.

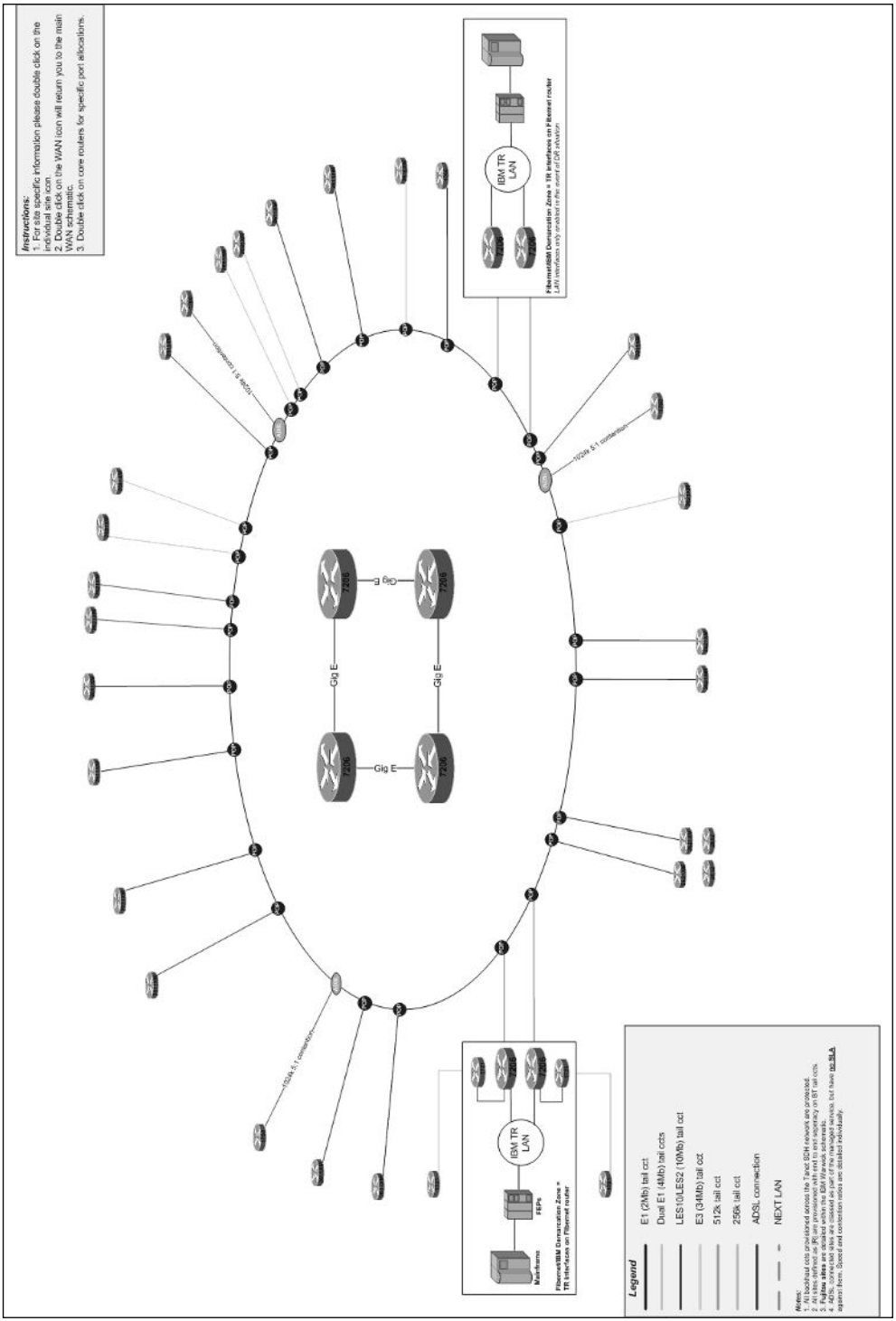


Figure 2.1 A Typical Network Topology Diagram

It is also advisable to try and gain a picture of where each of the network sites is located and how each of the links is utilized currently; although MOM is very low in terms of network utilization, a highly saturated link can cause potential problems with the flow of data from an agent to a management server or management server to database.

This information can also have a significant impact on how MOM is deployed in the environment.

Most larger organizations that run network analysis tools should be able to provide you with this information; if not, there are a number of free or low-priced solutions available online to aid you in this process.

This exercise is very important when deciding where your MOM components will be deployed, as there are certain network-related factors that need to be taken into consideration, for example, when deciding where to deploy management servers. That is, a large number of servers on a remote site with a high bandwidth link would most likely be managed by a centrally located management server, whereby a large number of servers on a remote site with a low bandwidth link would more than likely have a local Management Server deployed.

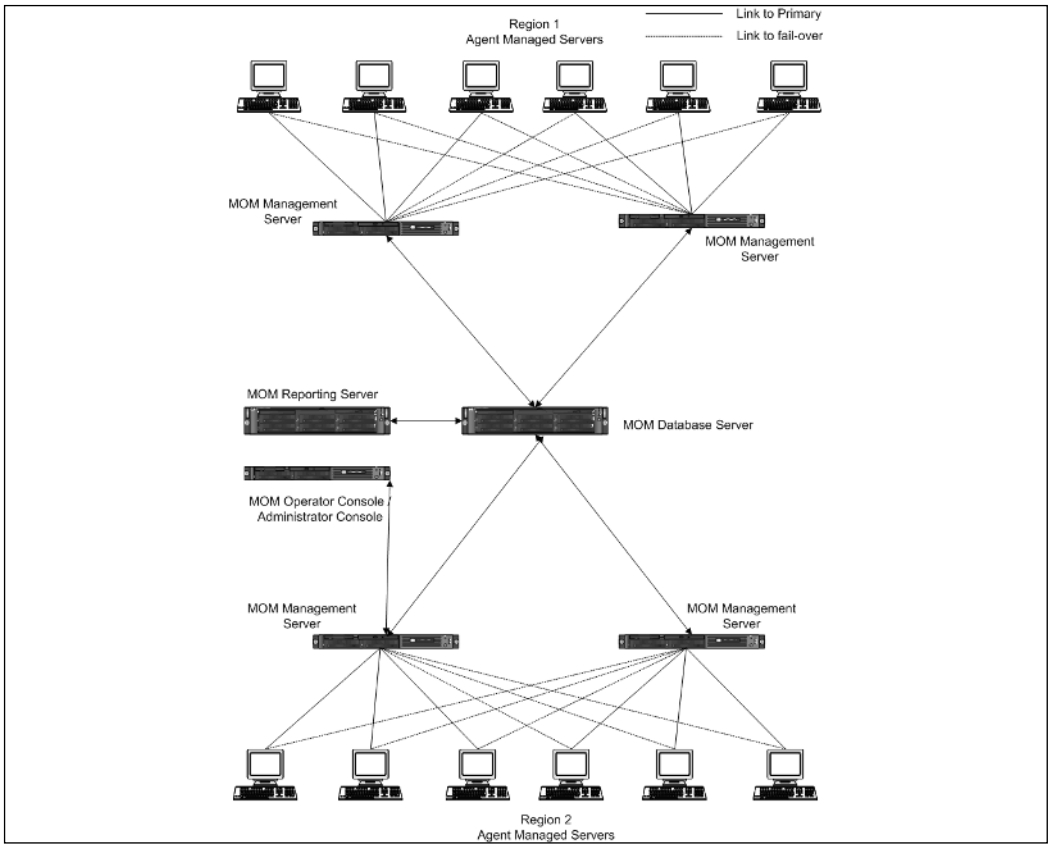
Another good practice is to try and create a simple diagram of how MOM will fit together within the local network topology such as is shown in Figure 2.2. This will allow you to play around with various architectural configurations during the planning stage until you find the right fit for your environment, and can also help when planning the necessary hardware you require for your implementation.

Hardware and Software Inventories

You will need to collect information regarding the hardware and software that resides on each of the servers that are potential targets for your MOM deployment; this will help you to analyze what the requirements might be for Management Packs, whether the server hardware and operating system will meet the minimum requirements for both the central MOM components and agents, and will also allow you to assess whether there may be any potential problems with deploying MOM in your environment, such as applications that may conflict with the MOM agent.

It is advisable to use any existing hardware and software inventory tool such as SMS to carry out this task, or if the operating system is running Windows Management Instrumentation (WMI), you can use scripts and a variety of third-party applications to collect this information. If none of these are available, then this (however painstaking) will have to be a manual process.

Figure 2.2 A Simple MOM Topology Diagram



You should be looking at collecting the following list of data from each machine:

- Location of the computer
- Number of processors it has, and the speed of each processor
- Amount of RAM
- Available disk space
- Video display (for MOM Consoles)
- BIOS settings
- Configurations for peripheral devices, such as printers
- Driver version numbers and other software and firmware information

You will also need to carry out a complete inventory of the applications that are installed on each of the target servers, including all custom (in-house) applications. Documenting the software installed on each computer will help you understand whether the target machine meets the MOM prerequisites and will allow you to identify the management packs that will need to be installed or created as part of the deployment.

For each target server in your organization, document the following:

- Applications that are installed
- Operating system that is installed
- Service packs that have been applied to the operating system
- Service packs that have been applied to applications

Microsoft Operations Manager 2005 Sizer

Now you have gathered some of the key information required to properly plan your deployment, it is important to assess what overhead MOM will place on your environment from both a hardware and network prospective. Microsoft provides many best practices that can be used to help you evaluate these factors.

To allow you to make a fairly accurate analysis of the performance and sizing of hardware systems and network links that will support MOM 2005, Microsoft provides a performance and sizing guide that is based on some of the lessons learned from deploying MOM internally at Microsoft and from some of the early deployments of the technology with customers. It is strongly recommended that you run through this guide prior to making any decisions on how MOM will be deployed in your organization. The key areas that this guide covers are:

- Large Agent Configuration—up to 5,000 agents
- Small Agent Configuration—up to 200 agents
- Single Agent Monitoring
- Agentless Monitoring
- MOM Connector Framework
- Reporting Server
- Low-Bandwidth Configuration

The guide walks you through a number of test scenarios that cover MOM 2005 performance and scalability, and can be used as a basis for carrying out testing of the product before MOM is moved to the pilot stage.

The guide is meant to be used in conjunction with the MOM sizing tool, which is available for download from Microsoft, and allows you to input figures gained from assumptions made from the guide or from your test environment.

The sizing tool is a Microsoft Excel spreadsheet that gives you information regarding the following key areas:

- Number of CPUs required
- Amount of memory required
- Disk space required for the MOM database
- Network utilizations at given line bandwidths

This tool can be very useful to allow you to get an initial idea of what effect MOM will have on your environment from both an infrastructure and a performance prospective.

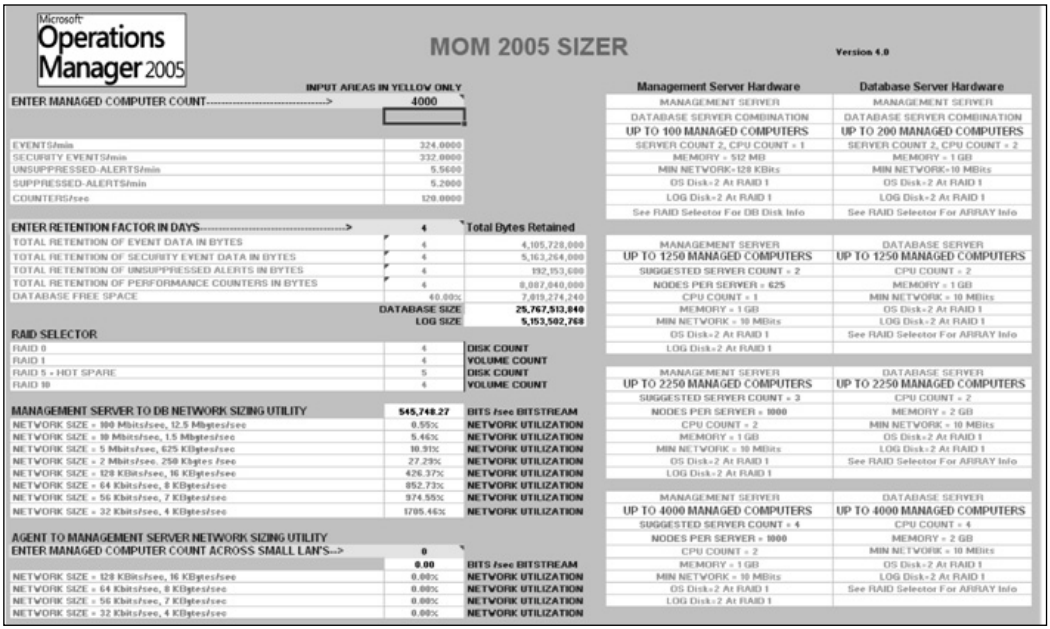
Figure 2.3 shows the first page of the MOM 2005 sizer; in the first yellow input field, enter the expected number of agents or managed computers that you plan to deploy MOM to and how long (in days) that you want to retain data in the operational database. The sizer then makes an estimate on how much data will be produced.

The sizer will estimate the number of events, alerts, and performance counters per second on the left side of the spreadsheet and provides recommendations for Management Server and Database Server hardware on the right as well as specific recommendations on disk array configuration.

The sizer also provides information about estimated network utilization between Management and Database Server, giving you valuable help in the design stage.

You can see in Figure 2.3 that a managed computer count of 4,000 has been entered with a retention time of four days; the sizer then recommends that the Management Server and Database Server are separated and that multiple Management Servers are deployed.

Figure 2.3 MOM 2005 Sizer



Microsoft Operations Manager 2005

MOM 2005 SIZER

Version 4.0

INPUT AREAS IN YELLOW ONLY

ENTER MANAGED COMPUTER COUNT----------> 4000

EVENTS/min	324.0000
SECURITY EVENTS/min	332.0000
UNSUPPRESSED-ALERTS/min	5.5600
SUPPRESSED-ALERTS/min	5.2000
COUNTERS/sec	120.0000

ENTER RETENTION FACTOR IN DAYS----------> 4 Total Bytes Retained

TOTAL RETENTION OF EVENT DATA IN BYTES	4	4,105,728,000
TOTAL RETENTION OF SECURITY EVENT DATA IN BYTES	4	5,163,264,000
TOTAL RETENTION OF UNSUPPRESSED ALERTS IN BYTES	4	192,153,600
TOTAL RETENTION OF PERFORMANCE COUNTERS IN BYTES	4	8,087,040,000
DATABASE FREE SPACE	40.00%	7,819,274,240
	DATABASE SIZE	25,767,513,840
	LOG SIZE	5,153,502,768

RAID SELECTOR

RAID 0	4	DISK COUNT
RAID 1	4	VOLUME COUNT
RAID 5 - HOT SPARE	5	DISK COUNT
RAID 10	4	VOLUME COUNT

MANAGEMENT SERVER TO DB NETWORK SIZING UTILITY	545,748.27	BITS /sec BITSTREAM
NETWORK SIZE = 100 Mbits/sec, 12.5 Mbytes/sec	0.55%	NETWORK UTILIZATION
NETWORK SIZE = 10 Mbits/sec, 1.5 Mbytes/sec	5.46%	NETWORK UTILIZATION
NETWORK SIZE = 5 Mbits/sec, 625 KBytes/sec	10.91%	NETWORK UTILIZATION
NETWORK SIZE = 2 Mbits/sec, 250 Kbytes /sec	27.29%	NETWORK UTILIZATION
NETWORK SIZE = 128 KBits/sec, 16 KBytes/sec	426.37%	NETWORK UTILIZATION
NETWORK SIZE = 64 Kbits/sec, 8 KBytes/sec	852.73%	NETWORK UTILIZATION
NETWORK SIZE = 56 Kbits/sec, 7 KBytes/sec	974.55%	NETWORK UTILIZATION
NETWORK SIZE = 32 Kbits/sec, 4 KBytes/sec	1705.46%	NETWORK UTILIZATION

AGENT TO MANAGEMENT SERVER NETWORK SIZING UTILITY

ENTER MANAGED COMPUTER COUNT ACROSS SMALL LAN'S--> 0

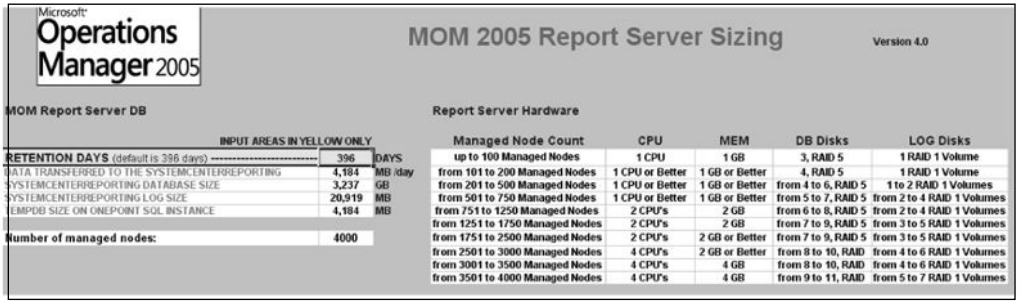
	0.00	BITS /sec BITSTREAM
NETWORK SIZE = 128 KBits/sec, 16 KBytes/sec	0.00%	NETWORK UTILIZATION
NETWORK SIZE = 64 Kbits/sec, 8 KBytes/sec	0.00%	NETWORK UTILIZATION
NETWORK SIZE = 56 Kbits/sec, 7 KBytes/sec	0.00%	NETWORK UTILIZATION
NETWORK SIZE = 32 Kbits/sec, 4 KBytes/sec	0.00%	NETWORK UTILIZATION

Management Server Hardware	Database Server Hardware
MANAGEMENT SERVER	MANAGEMENT SERVER
DATABASE SERVER COMBINATION	DATABASE SERVER COMBINATION
UP TO 100 MANAGED COMPUTERS	UP TO 200 MANAGED COMPUTERS
SERVER COUNT 2, CPU COUNT = 1	SERVER COUNT 2, CPU COUNT = 2
MEMORY = 512 MB	MEMORY = 1 GB
MIN NETWORK=128 KBits	MIN NETWORK=10 MBits
OS Disk=2 At RAID 1	OS Disk=2 At RAID 1
LOG Disk=2 At RAID 1	LOG Disk=2 At RAID 1
See RAID Selector For DB Disk Info	See RAID Selector For ARRAY Info
MANAGEMENT SERVER	DATABASE SERVER
UP TO 1250 MANAGED COMPUTERS	UP TO 1250 MANAGED COMPUTERS
SUGGESTED SERVER COUNT = 2	CPU COUNT = 2
NODES PER SERVER = 625	MEMORY = 1 GB
CPU COUNT = 1	MIN NETWORK = 10 MBits
MEMORY = 1 GB	OS Disk=2 At RAID 1
MIN NETWORK = 10 MBits	LOG Disk=2 At RAID 1
OS Disk=2 At RAID 1	See RAID Selector For ARRAY Info
LOG Disk=2 At RAID 1	
MANAGEMENT SERVER	DATABASE SERVER
UP TO 2250 MANAGED COMPUTERS	UP TO 2250 MANAGED COMPUTERS
SUGGESTED SERVER COUNT = 3	CPU COUNT = 2
NODES PER SERVER = 1000	MEMORY = 2 GB
CPU COUNT = 2	MIN NETWORK = 10 MBits
MEMORY = 1 GB	OS Disk=2 At RAID 1
MIN NETWORK = 10 MBits	LOG Disk=2 At RAID 1
OS Disk=2 At RAID 1	See RAID Selector For ARRAY Info
LOG Disk=2 At RAID 1	
MANAGEMENT SERVER	DATABASE SERVER
UP TO 4000 MANAGED COMPUTERS	UP TO 4000 MANAGED COMPUTERS
SUGGESTED SERVER COUNT = 4	CPU COUNT = 4
NODES PER SERVER = 1000	MEMORY = 2 GB
CPU COUNT = 2	MIN NETWORK = 10 MBits
MEMORY = 1 GB	OS Disk=2 At RAID 1
MIN NETWORK = 10 MBits	LOG Disk=2 At RAID 1
OS Disk=2 At RAID 1	See RAID Selector For ARRAY Info
LOG Disk=2 At RAID 1	

This spreadsheet also includes a MOM 2005 Reporting sizer, which enables you to perform similar sizing tasks for your reporting server (see Figure 2.4). The only data that you are required to input on this sheet is how long you wish to retain data on your reporting server. The default value is 396 days and it utilizes the agent data calculated in the previous sheet. Again, projected data figures are provided, along with recommended hardware specifications and disk array configuration.

There is no consideration of network bandwidth in this sheet as the data can be transferred out of business hours or at times when appropriate bandwidth is available.

Figure 2.4 MOM 2005 Report Server Sizing



Microsoft Operations Manager 2005

MOM 2005 Report Server Sizing

Version 4.0

MOM Report Server DB

INPUT AREAS IN YELLOW ONLY

RETENTION DAYS (default is 396 days) ----------	396	DAYS
DATA TRANSFERRED TO THE SYSTEMCENTERREPORTING	4,184	MB /day
SYSTEMCENTERREPORTING DATABASE SIZE	3,237	GB
SYSTEMCENTERREPORTING LOG SIZE	20,919	MB
TEMPDB SIZE ON ONEPOINT SQL INSTANCE	4,184	MB
Number of managed nodes:	4000	

Report Server Hardware

Managed Node Count	CPU	MEM	DB Disks	LOG Disks
up to 100 Managed Nodes	1 CPU	1 GB	3, RAID 5	1 RAID 1 Volume
from 101 to 200 Managed Nodes	1 CPU or Better	1 GB or Better	4, RAID 5	1 RAID 1 Volume
from 201 to 500 Managed Nodes	1 CPU or Better	1 GB or Better	from 4 to 6, RAID 5	1 to 2 RAID 1 Volumes
from 501 to 750 Managed Nodes	1 CPU or Better	1 GB or Better	from 5 to 7, RAID 5	from 2 to 4 RAID 1 Volumes
from 751 to 1250 Managed Nodes	2 CPU's	2 GB	from 6 to 8, RAID 5	from 2 to 4 RAID 1 Volumes
from 1251 to 1750 Managed Nodes	2 CPU's	2 GB	from 7 to 9, RAID 5	from 3 to 5 RAID 1 Volumes
from 1751 to 2500 Managed Nodes	2 CPU's	2 GB or Better	from 7 to 9, RAID 5	from 3 to 5 RAID 1 Volumes
from 2501 to 3000 Managed Nodes	4 CPU's	2 GB or Better	from 8 to 10, RAID	from 4 to 6 RAID 1 Volumes
from 3001 to 3500 Managed Nodes	4 CPU's	4 GB	from 8 to 10, RAID	from 4 to 6 RAID 1 Volumes
from 3501 to 4000 Managed Nodes	4 CPU's	4 GB	from 9 to 11, RAID	from 5 to 7 RAID 1 Volumes

The MOM 2005 sizer tool should give you a good starting point for assessing the impact of your MOM deployment. The information contained within the tool was taken from tests carried out against Microsoft's internal implementation of MOM and from around 34 customers who were early adopters of the technology in their production environment running MOM from the initial beta through to release. These customers were of all sizes, from small businesses to large enterprises and from different types of businesses such as banks, public sector, and manufacturing. Their feedback was very vital in providing a real-world element to the guidance offered by the sizing tool.

Best Practices According to Microsoft

- You may find it helpful to choose a deployment planning methodology, or framework, to help you through the planning and deployment of MOM. For more information about the Microsoft Solutions Framework, see www.microsoft.com/technet/itsolutions/msf/default.mspx.
- In addition to the MOM-specific planning guidance provided in this guide, consider using the information and job aids included in the *Windows Server 2003 Deployment Kit*.
- An essential read for this stage of the project is the *Microsoft Operations Manager 2005 Deployment Planning Guide*. This guide provides you with a roadmap for developing a deployment plan for your MOM 2005 deployment. In addition, this guide directs you to the relevant conceptual, security, and planning resources you might need to help you develop a sound deployment strategy.

Some Independent Advice

The MOM 2005 sizer is meant only as a guideline to performance and utilization figures, and should always be backed up by your own testing. The sizer bases its figures on a low number of management packs; these figures will obviously be inaccurate as you increase the number of management packs deployed. Network traffic can also vary in different organizations depending on numbers of Exchange Servers and Domain Controllers, for example.

Shortcuts…

Getting Buy-in

Get early buy-in with MOM from the different teams that you will talk to by highlighting how it will benefit their particular areas; for example, with a network team MOM can help identify network versus application issues very quickly, saving arguments between teams, and with application teams MOM can allow them to have their own view of the operation of the application such as a SQL team having a scoped view of their SQL servers.

This will make evaluating the environment a much easier task as people will be happy to help you collect information about their prospective areas.

Identifying Requirements

It is recommended that you make a list of your requirements in order of their priority to your organization.This will allow you to focus your initial MOM design on the essential requirements to ensure that key functionality is delivered in the first phase.

In accordance with Microsoft Solution Framework best practices, these requirements must be:

- Specific
- Measurable
- Achievable
- Results-oriented
- Time-specific

It is good to establish metrics for measuring your success which must be achievable within your allotted time and in line with the established budget. If you follow these simple guidelines they will help you in establishing and tracking achievable project milestones which means you will be well on your way to a successful implementation.

Security Requirements

There are a number of Security requirements that need to be taken into account that can affect your MOM deployment, these will need to be researched and planned for prior to embarking on your design phase.

You need to make sure that you have sufficient privileges with which to deploy MOM in your environment; to install MOM correctly you need to be an administrator on all servers that you will be installing MOM components on. You also need to make sure that you have sufficient privileges to be able to create a new database on your database server. In the situation where you are utilizing an existing SQL Server instance, for example, it is likely that SQL server security has been set up by someone else, so make sure that you check with the SQL DBA or person responsible for that server first.

You will also need to understand who has access to your network and what levels of privilege they have on your servers; for example, members of the Domain Administrators group automatically have full MOM Admin privileges on Management Servers, so you will not need to add these users to any MOM Security groups you require. Also, if you are planning on deploying to non-Windows platforms or network devices make sure that you understand how access permissions are set up. This can save a lot of time later down the line.

If your organization is a strong user of group policies make sure you have a firm understanding of how your servers are locked down and what policies are applied to them. Many MOM installations have problems if, for example, Domain or Local System Account access has been restricted.

If MOM is to be used across a company firewall, it is very important to understand how these are configured; MOM uses TCP and UDP 1270 to communicate through firewalls, so it is good to get these ports configured very early on in your project, especially if your organization practices strict change control procedures that may delay agent roll-out later down the line.

You need to understand what level of MOM security is acceptable for the organization. Some companies have strict control on the use of service accounts and may opt for an agent action account with the minimum level of permissions required to operate (low privilege). For example, on Microsoft Windows Server 2003, the MOM Service can run under the Network Service account. This account has lower permissions than the Local System account and enhances the security of the MOM Service.

MOM 2005 also comes with a number of built in security features that allow for more secure agent/server communication:

You will also need to decide whether Mutual Authentication needs to be enabled; this requires that the computer account of the agent communicating with the MOM Management Server has a valid Active Directory account.

This is a global setting within MOM so if any of the computers that you plan to deploy agents to, are behind a firewall or in a non-trusted domain then this needs to be set to disabled when installing the Management Server and during agent installs.

You also need to know whether any legacy MOM 2000 or MOM 2000 sp1 clients will be connecting to your new management servers, for example, during a rolling upgrade, as this will also need to be deselected as part of the post-install configuration.

Another MOM security requirement is whether you will be allowing custom responses to run on your management server which are triggered by rules generated on your managed servers, these could be:

- Script responses configured to be launched on the Management Server
- Notification responses when a command is specified
- Command/batch file responses configured to be executed from the Management Server

NOTE

You may well not know this exact information at this stage, so it may best leaving the default setting of disabled to begin with.

Other MOM security features will be discussed later in this book.

It is also good practice at this stage to draw up a list of people who will require access to MOM from both an administrative and a user aspect, this will allow you to build this into your deployment plan. An administrative user will generally be involved with the day to day management of MOM whereby a user would be involved with the day to day management of alerts. Finally, you will a need to find out if the organization has naming standards in place for service accounts and domain user groups, as these can be drawn up and specified during your design proposal.

Business Requirements

You must understand what the true business requirements are that are driving the project. This involves speaking to people across the organization who are involved

with delivering and supporting IT from a business prospective. This could include the CFO, IT managers, or directors and business process owners.

The kinds of questions that you should be asking are:

- What does the business expect from MOM?
- What does the business expect from its investment in the technology?
- What are the business drivers for the monitoring of the IT infrastructure (cost savings, better uptime, and more accountability from the IT department)?
- What are the critical line of business (LOB) systems and applications that need to be managed (Active Directory, messaging applications, and third-party solutions)?
- What are the key business indicators for a successful implementation of MOM (valid reports, fixes to existing problems, and application and service views)?

The idea of this exercise is to evaluate what the business criteria are for the project and to compare this against the technical requirements.

Many IT projects fail because these factors are not taken into consideration and the end result is something that reflects only the technical needs of the business.

Even though the organization you are working with or for already may have made both a financial and technical commitment to MOM, it is important to still constantly sell the benefits of the product. This will help you get the most from it in the long term and will certainly help you out in terms of quality of information in both the evaluation and planning stage of the project.

It may help if you start each of your interviews with a high-level overview of MOM, explain how it works, and explain how it will aid the organization moving forward. This often can provoke good questions and can stimulate quality answers that will enable you to get the most from this time spent.

It can help in this business evaluation stage if the people you talk to fully understand the reasons for using MOM and how it can impact the business in a positive way.

A good tool to help you present the business benefits of MOM is available from a company called CIOView (www.cioview.com/products/prod_mom.html). This is an ROI calculator that can help both consultants and technical engineers understand and measure the financial impact of Microsoft Operations Manager 2005; evaluate what the likely costs and benefits will be in the short and long term; automatically generate the key financial metrics such as ROI, IRR, NPV, and Payback Period; and

subsequently build a picture of how MOM impacts the business financially (see Figures 2.5 and 2.6).

Figure 2.5 MOM ROI Benefit Summary

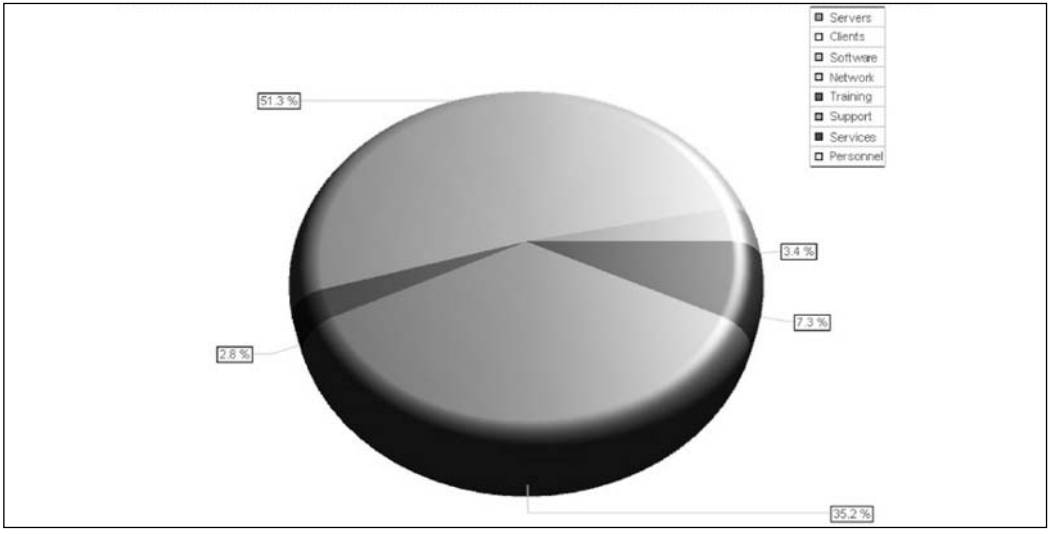
Accounting Basis

What accounting basis do you wish to use when presenting your benefit summary? Project Timeline Accounting

Benefit Summary

	Include?	Initial	Year1	Year 2	Year3	Year 4	Year 5
Timeline			7/1/05-6/31/06	7/1/06-6/31/07	7/1/07-6/31/08	7/1/08-6/31/09	7/1/09-6/31/10
End-user Time Savings	☑	$0	$3,902	$4,233	$4,579	$0	$0
IT Personnel Savings	☑	$0	$222,127	$240,977	$260,650	$0	$0
Operational, Hardware, and Software Savings	☑	$0	$48,474	$52,588	$56,881	$0	$0
Revenue and Security Benefits	☑	$0	$0	$0	$0	$0	$0
Total Benefit		$0	$274,504	$297,798	$322,110	$0	$0

Figure 2.6 MOM ROI Benefit Graph



A good practice for collecting this business-related data is to design a spreadsheet listing the business requirements that can then be compared against the technical requirements, allowing you to make a balanced assessment on what MOM needs to be able to deliver in your environment (see Table 2.1).

Table 2.1 Comparing Business and Technical Requirements

Business Requirement	Technical Requirement
Decreased running costs	Better understanding of application and OS failures
Less downtime	Distribution of support functions
Better visibility of IT through reporting	Consolidation of management tools
Accountability	Better SLA response times

Some of these requirements can turn out to be very similar, and you should be able to come up with a list of the top five to 10 requirements, allowing you to focus the first stages of the project around what is really needed by both the business and technical side of the organization.

Technical Requirements

It is important also to understand the technical drivers for deploying MOM; often these can differ a great deal from what the business needs are.

For this exercise you will need to talk to the people within the organization who are responsible for implementing, managing, and supporting the IT infrastructure. This could include IT managers, infrastructure owners, and IT support personnel.

There are a number of questions that you need to ask at this stage, and certain information that you will need to gather for the planning stage, including the following.

What Is the Technical Support Model?

- Is there first-, second-, or third-line support?
- What are these support teams called, and how are they involved with problem resolution and escalation?

This information is particularly useful when configuring MOM for alert handling.

Is There a Corporate Helpdesk Product in Use, and Does This Drive the Support Operation?

- Which helpdesk product is in use?
- Has there been any customization carried out on it to bring external sources of data in?

- Is the IT support operation driven by this ticket system?

This information can help decide how MOM will fit into the support operation.

Tip: MOM 2005 comes with its own connector framework (MCF), which allows you to connect directly to other third-party management platforms, applications, or helpdesk products using some simple XML-based commands. If the organization you are working with already has an advanced support infrastructure in place, then seriously consider hooking MOM into it. This ensures that MOM alerts will be handled correctly by the right personnel, and saves a great deal of configuration work with MOM later down the line.

Microsoft has written an excellent white paper for Service Desk implementation called the *Auto-ticketing Solution Accelerator*, which provides guidance for automated ticket generation, enabling the automated posting of a request (or ticket) into the Trouble Ticketing (TT) system used for incident management (http://go.microsoft.com/fwlink/?LinkId=33876&clcid=0x409).

There are also a number of very good third-party MOM connectors available for helpdesk\service desk integration such as the IWAVE adapter from Skywire, which is an out-of-the-box connector for many of the well-known brands of service desk such as Remedy, Clarify, and Peregrine Service Center, which not only provides integration via the Microsoft Connector Framework (MCF), but also has built-in workflow for more advanced ticket processes and for guaranteeing delivery (www.skywiresoftware.com/Pages/Products.aspx?s=integration_iwaveintegrator_overview&c=6&p=36).

What Is the Monitoring Scope?

- How many servers are to be included in the pilot stages and future stages of the deployment?
- What applications need to be monitored now and in the future?

What Information Is Required for MOM Topology?

- Is fault tolerance and redundancy required?
- Is the necessary hardware available to support the configuration?
- What are the technical reporting requirements?
- How many consoles are required to support and manage MOM?

- Is the Microsoft Connector Framework (MCF) required for integration into other platforms?
- Is there a requirement to multitier management groups or multihome agents?

What Information Is Required for Accurate Design Configuration?

- What are the server locations?
- What should the Management Group name be?

What Management Packs Are Required?

It is good to try to build an initial list of what applications and services need to be monitored with MOM. This list can start off extremely large, as many of the people you talk to such as technology or application owners all will have their own requirements in their particular areas. Although it is important to sell MOM's capabilities to each of these people that you meet, remember that the most successful MOM implementations start off with a very focused set of Management Packs in the early stages of the deployment, with additional packs being added once MOM has been bedded in.

What MOM Alert Mechanisms Are Required?

- If E-Mail notification is required, what mechanism is available (e.g., MAPI, SMTP)?
- Does the organization have a paging or Short Message Service (SMS) text messaging service available?
- Who needs to be notified and when?
- Who will be responsible for the administration of Alerts?
- What backup mechanisms are there in the case of a failure of the primary alert mechanisms?

At the end of this exercise you should have a good idea of the initial scope required for your deployment as well as enough information with which to put together a good design plan.

User Requirements

You will need to gather a list of requirements from within the organization, about the users that will be using MOM on a day-to-day basis. This could include basic console access security, scopes, and views that users will be given, and also any necessary access to reports that is desirable.

Basic user access to the MOM console is broken down into four areas, which we will discuss next.

MOM Administrators

The members of this group can perform any task in MOM 2005 in either console, except reporting functions. To perform these functions they must also be a member of SC DW Reader group. The MOM Administrators group is created only on the MOM Management Server and has no members by default (for new installations). MOM administrators should be made a member of this group as it gives access to all aspects of the product.

Note: Members of the local administrators group of the Management Server can also perform all MOM operations as if they were members of the MOM Administrators group.

MOM Authors

The members of this group can import, export, create, and modify management packs in the MOM Administrator console. They can also use the Operator console and perform any task in it. They cannot change which computers are managed or the type of management used. This group is created only on the MOM Management Server and has no members by default (for new installations).

This group typically is populated with management pack owners or people who need to write their own rules and responses.

MOM Users

The members of this group can use any Operator console functionality on any computer that belongs to the scope associated with the MOM Users group. They cannot, however, perform runtime tasks. They are limited to using the Operator console and do not have access to the Administrator console, except to use it to open the Operator console. This group is created only on the MOM Management Server and has only the DAS account as a member by default (for new installations).

This is the standard user group for MOM; any users not involved in the day-to-day configuration of MOM should be added to this group.

SC DW Reader

The members of this group have access to the SQL Server Reporting Services on the MOM Reporting Server and can perform reporting functions, such as creating, viewing, and saving reports. Members of this group are given permission to perform the archiving (DTS) operation. This group is created on the MOM Reporting Database Server and has no members by default (for new installations).

This group provides standard access to MOM's reporting capability; further security can be implemented using the built-in security mechanism in the Report Servers SQL Server Reporting Services console.

Once you have a list of what users will go into which groups, it is good to establish if any console scoping or custom views is required.

MOM 2005 allows for the creation of customized views, for example, to restrict a specific user to access and manage only a certain subset of computer groups. Scoping can be used to isolate users, preventing them from seeing and acting on each other's systems. Typical uses for this are to restrict a view by a local site, or for specific application or service owners who only want to see the servers relating to their area of management.

There may also be a need to create customized views for the environment that reflect certain types of data; for example, alerts appearing within a certain time period or events relating to a specific application action.

Best Practices According to Microsoft

Planning for security is imperative in any deployment scenario. It is important to clearly document the security features and requirements in your project plan. For more information about MOM 2005 Security, see the *Microsoft Operations Manager 2005 Security Guide*, and refer to it often while planning your MOM deployment.

Some Independent Advice

The Management Group name is very important to the overall MOM design and cannot be changed easily without reinstalling the product. This needs to be unique and should take into account the fact that the number of Management Groups could change at a future date due to mergers with other environments that already have MOM installed, which could mean two Management Groups being connected together.

A typical MOM Management Group name, for example, could be MOM-ACME-01 or ACMEMOM01.

The MOM Agent Action Account will work perfectly fine under the Local System account for nearly all of the Microsoft Management Packs and a lot of the third-party management packs, so if the customer does not have an issue with this account being used to run rules and responses on the target server, then it is far easier utilizing the security credentials of this account. The "low-privilege scenario" requires not only the creation of certain rights on each target server but also individual configuration of rights for each management pack, which can cause a great deal of work later on in the deployment.

As each of the Management Packs required has a different set of requirements from both a security and reporting standpoint, it is advisable to study each Management Pack's respective guide, as this will have a bearing on how you plan your security in the design stage of your implementation.

Make sure your security team understands how MOM will affect the environment and make any necessary changes to group policies or firewalls before you deploy any components.

Shortcuts…

Universal Groups

You can lower administration overhead of MOM's local security groups by creating domain-wide, or universal, groups and adding these groups to the appropriate MOM group. This way you can manage the members of these groups universally.

Selecting a Version of Microsoft Operations Manager

MOM 2005 comes in two specific versions, Enterprise and Workgroup Edition. MOM 2005 Workgroup edition has all the same core components as Enterprise, but runs on MSDE rather than fully blown SQL, so it has a database limit of 3GB as

well as support for up to 10 agents only. It does not include reporting or the MCF connector for multitiering of management groups, and all the components must be installed on the same server. It does have access to the same Management Packs as it bigger brother however, and comes preinstalled with the most commonly used ones.

Because of the restrictions of the product, it is designed for very small environments only or for use by specific product teams who just want to manage a small number of application servers. It is also very cheap, can be bought off the shelf, and is ideal for piloting MOM so you can get a very basic feel of its capabilities.

For any organization planning on rolling MOM out to more than 10 servers, the Enterprise Edition should be selected.

Summary

To ensure a successful implementation of Microsoft Operations Manager in your environment, you will need to do a thorough assessment of your environment to ensure that you plan your design and implementation correctly.
In this chapter we have looked at the key areas that you need to be collecting data about, we have talked about ways in which we can collect this information, and have discussed various questions that you can ask to help you get this information from various parts of the organization. We also have looked at how you identify requirements from a security, business, technical, and user standpoint as well as some information on selecting the right version of MOM for your environment.

Evaluating your environment can be one of the more time-consuming exercises in the implementation of MOM in your organization; however, it is also one of the most critical ones. Get the right information by asking the right questions, and collecting accurate data can really be the key to the success of your project.

As this stage will bring you to many different areas of the business, it will also give you a chance to truly understand how MOM will impact everyone, and will also allow you to sell MOM's great capabilities to the people you meet.

Make sure that you read all the documentation detailed in this section thoroughly and try and stick to the best practices, and you should be ensured of a smooth ride into production with MOM.

Understanding Your Environment

- ☑ You need to collect accurate data regarding key network data such as existing network protocols, network bandwidth, and network hardware such as routers, switches, and firewalls.

- ☑ Make sure you either get hold of or create good network topology diagrams.
- ☑ Collect configuration information on hardware you will deploy MOM components to.
- ☑ Collect version and configuration data on operating systems and applications, including service packs and hotfix information.
- ☑ Use the MOM 2005 sizer to assess the impact MOM will have on your environment.

Identifying Requirements

- ☑ Make a list of requirements in order of priority and focus on achievable milestones based on project constraints.
- ☑ Understand how your organization approaches and deals with security and make sure that anything that will affect your MOM deployment is sorted out before you embark on the implementation.
- ☑ Speak to as many areas of the business as possible that may be affected by your MOM deployment, this should include both technical and non-technical people.
- ☑ Draw up a list of business versus technical requirements and evaluate both factors, the most successful MOM deployments are ones that meet as many requirements from both of these areas as possible.

Selecting a Version of Microsoft Operations Manager

- ☑ MOM Workgroup Edition is designed for very small organizations of 10 servers or less and has no reporting or Microsoft Connector Framework component.
- ☑ MOM Workgroup is ideal for monitoring small numbers of Application servers such as SQL or IIS or as a starter product for your environment as it is capable of running all Microsoft Management Packs.
- ☑ If your deployment will incorporate more than 10 servers or if reporting is a priority then you need to start with the Enterprise edition.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: When evaluating my environment what are the key areas of my infrastructure that I need to understand?

A: You, need to have a thorough understanding of both the network topology and software and hardware configuration of all servers you will install MOM components on to.

Q: What tools area available to help me assess what impact MOM will have on my environment?

A: Microsoft provide both a performance and sizing whitepaper and a database sizing tool, these will allow you to get a good estimate on the overall impact of your MOM deployment on your infrastructure.

Q: I have many parts of my organization who would like their specific service or application monitored and I am worried that the project is going to be too large, are their any risks?

A: You need to keep your initial deployment very focused, so draw up a list of requirements and prioritize on what is critical to you now. AD and Exchange are quite often the two core applications in most organizations so start here, get your infrastructure and support processes right, then you can expand your implementation to cover other areas, the biggest single reason for most MOM deployments failing is loading too many management packs into MOM at an early stage.

Q: I have a number of agents behind firewalls, what ports do I need to get my network team to open in preparation for my deployment.

A: MOM uses TCP and UDP ports 1270 for agent communication and heart-beating. You will have to manually install the agent with the control level set

FAQ

to "None" and any updates to the agent such as service packs will have to be installed manually.

Q: I plan to manage some servers in nontrusted domains. How will this affect the configuration of MOM?

A: You will need to make sure that you disable mutual authentication in global setting on your management servers and during agent deployment.

Q: I am struggling to get all the financial backing I need to deploy MOM fully in my environment. What can I do to convince my CFO to give me more funding?

A: MOM can deliver extremely high ROI to any organization in a short period of time. Create a simple spreadsheet highlighting some of the obvious business benefits or use a tool like CIOViews ROInow for MOM to produce graphical charts of cost savings.

Q: We have made a significant investment in our company's service desk product, which allows us to operate completely to ITIL standards and therefore fully drives our support operation. Won't MOM be another process that sits outside of this?

A: Not at all. MOM comes with a built-in connector framework that will allow you to hook MOM into your existing processes. There are also some excellent third-party connectors such as Skywire's IWAVE connector for MOM, which has a number of ready-made helpdesk adapters.

Q: I need to monitor only eight servers in my part of the organization. Do I need to buy the full version of MOM?

A: No, Microsoft has created a Workgroup edition of MOM designed for smaller organizations. It has some limited functionality, but will allow you to utilize all of Microsoft's Management packs and many of the third-party management packs.

Chapter 3

Planning a MOM 2005 Deployment

Solutions in this chapter:

- **Planning Your MOM Topology**
- **Planning for Features and Configurations**
- **Planning for Users**
- **Security Requirements**
- **Disaster Recovery Planning**
- **Advanced Configurations**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

Taking the time to plan your deployment of Microsoft Operations Manager (MOM) 2005 and architect a solution that meets the goals of your organization or your customer is critical to the success and speed of the deployment. In this chapter, we will start with a review of the key components that make up a MOM architecture, followed by an overview of the planning process where we will explore capacity planning, redundancy planning, and configuration planning. Once you have a grasp of the type of planning that is required and the information that is needed to make the appropriate decisions, we will look at some of the tools available to assist you with your planning. With the architectural planning piece behind you we will shift our focus to operational planning, where we will look at security requirements, including planning for users and delegated administration, as well as disaster recovery planning. We then will wrap things up with a look at the five Solution Accelerators, which can provide you with technical and prescriptive guidance with more advanced configurations. This chapter will help prepare you for Chapter 4, which focuses on performing the installation.

Planning Your MOM Topology

Planning your Microsoft Operations Manager 2005 deployment is not a difficult task, but is one that should be approached with an open mind and an inquisitive attitude. The goal of the planning process is to create an architecture that meets the goals of the organization both today and over the life of the product and that provides the ability to scale and grow the implementation to meet the organization's changing requirements. The planning process usually is approached from one of two perspectives: that of an internal corporate employee or that of a contractor brought in to facilitate the implementation based on his or her expertise. Regardless of the perspective, the end goal remains the same. The key difference is that the consultant usually needs to spend some extra time getting to know the business, its processes, and technical environment in order to develop a solution that truly meets the goals of the organization.

MOM Components

Microsoft uses a number of different icons both in the Microsoft Operations Manager 2005 product as well as in their publicly available and ever-growing documentation to represent the different components available in MOM 2005. Figure 3.1 illustrates the icons used to represent the five core MOM 2005 components.

Figure 3.1 Core MOM 2005 Components

The first icon on the left-hand side of Figure 3.1 represents the database. In MOM 2005, the database is the central repository that contains all operations data as well as all the configuration information for your management group.

Operational data stored in the MOM 2005 OnePoint database includes the information collected by the MOM agents (events, alerts, and performance data) and forwarded to the MOM Management Server, which in turn sends this operational data to the MOM database.

Configuration information relates to the settings, both default and customizations that you have defined for your MOM environment through the MOM Administrator console. Included would be settings such as the rules that monitor your environment, agent-related information, MOM Management Server information, such as global settings like security, custom alert fields, alert resolution states, communications, e-mail server, notification command format, and whether Service Pack 1 for MOM 2005 has installed licenses. Essentially, all configuration changes that you make through the MOM Administrator console will be stored in the MOM 2005 OnePoint database.

The second icon from the left represents the MOM Management Server. The Management Server in MOM 2005 is the central connection point in MOM for all the MOM agents and was formerly referred to as the Distributed Consolidator Agent Manager (DCAM) in MOM 2000. The MOM Management Server is effectively the communication broker between the agents that collect monitored information and the database that stores that information. Your MOM agents will never communicate directly with the MOM database; they will always communicate with the MOM Management Server, which in turn communicates with the database. The user interfaces, which include the Web, Administrator, and Operator consoles, all talk to the Management Server.

The Management Server can play a single role in your MOM architecture and act solely as a Management Server (which is the recommended configuration in large enterprise deployments with more than 300 monitored agents), but it can also

be configured to host other components. These other components include the Web Console Server, which is an IIS Web site depicted in the middle icon in Figure 3.1, or the Microsoft Connector Framework (MCF), a Web service written in managed code that can be used to connect MOM 2005 with other management products like Tivoli or HP OpenView. This component is depicted in Figure 3.1 as the second icon from the right. The MCF can also be used to connect multiple MOM management groups together in a parent/child configuration using the MOM-to-MOM Product Connector (MMPC), allowing a single parent management group to have up to 10 child-management groups reporting to it. All or a combination of these components can be installed on the Management Server, providing you with a great deal of flexibility in how you configure your MOM environment. The other benefit to you is that you can start with a simple configuration and add on these optional components as they become required.

The last of the MOM components shown in Figure 3.1 is the File Transfer Server, which sometimes is used in response to upload or download files. One example of where this component is used quite frequently is with the Microsoft Baseline Security Analyzer (MBSA) Management Pack (MP), where it is used to transfer new versions of the mssecure.cab file from a central location to all the agents that are configured to use the MBSA MP.

NOTE

MBSA is a free utility available from Microsoft that allows you to scan one or more computers running Microsoft Windows® Server 2003, Windows XP, Windows 2000, or Windows NT® 4.0 for common security misconfigurations. The MBSA utility can be deployed to some or all of your MOM agents as a part of the MBSA management pack. This can be a not-so-pleasant surprise if you are not expecting this.

Before we move on to the different types of monitored computers, it's important to understand another term that isn't represented in any of the figures you have seen so far, the concept of a management group. A management group, formerly referred to as a configuration group, is made up of a single MOM OnePoint database, one or more MOM Management Servers, and one or more monitored agents. The extent to which you can grow a single management group will be touched upon later in this chapter, but for now, the focus is simply on what this refers to. As you grow a management group through the addition of a second management server, you must

manually balance the monitored agent load between the two MOM servers but the second MOM server helps to address the issue of redundancy. Because all the configuration data for MOM is stored in the database and all MOM management servers within the same management group share a single OnePoint database, this configuration information stored within the database is shared as well.

Monitored Computer Types

Now that you have a better understanding of the various MOM components available to you, let's turn our attention to the different types of monitored computers. There are three different options available to monitor computers in MOM 2005. These include agent-managed, agentless, and unmanaged systems; the icons representing each of these can be seen in Figure 3.2.

Figure 3.2 MOM 2005 Monitored Computer Types

The key difference between the managed computer types is that agent-managed computers require that an agent be installed. This can be accomplished through a manual installation at the client or through the automated installation features within the MOM Administrator console. The distribution and installation of the MOM agent software can also be managed via Group Policy, Systems Management Server (SMS), or a third-party software distribution application.

Agentless monitored systems are computers that you wish to manage but that you do not want, or are not able, to install an agent on. Each management server can support up to 10 agentless monitored servers with up to 60 agentless monitored servers in a single management group. Don't be confused by the term agentless, because an agent does actually get installed—but it is installed on the management server as opposed to the actual monitored system. The installation of additional agents on a management server that is used to perform remote monitoring significantly increases the load on the management server and degrades performance, so use this type of monitoring with caution. One example of where agentless monitored systems can be used is with Windows NT 4.0 servers. It's not uncommon for

large organizations to still have a small collection of Windows NT 4.0 Servers, and because a MOM 2005 agent cannot be installed on a system running Windows NT 4.0, this type of system might be a candidate for agentless management.

Another consideration with agentless monitoring is communication between the management server and the agentless monitored system. This communication uses RPC port (TCP 135) and the DCOM port range. Therefore using agentless monitoring for systems outside a firewall is not supported. The management server's Action Account must also be a local administrator on the remote computer if you want to use agentless monitoring, meaning that they must either be in the same domain or a trust relationship must exist between their domains.

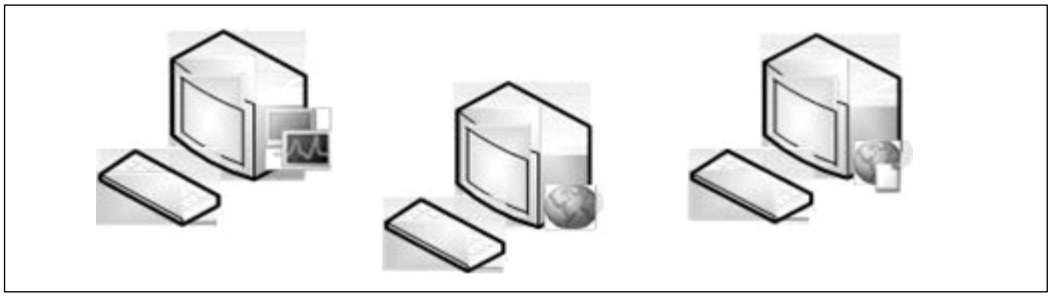
TIP

Always read the MP configuration guides that come with each of the Microsoft MPs to learn about their specific configuration requirements. This will alert you to issues with potential configuration requirements. For example, the IIS Management Pack does not support agentless monitoring because monitoring IIS servers requires that the MOM agent have administrative rights to the IIS metabase.

Consoles

MOM 2005 also provides four different management consoles, the fourth provided with the installation of MOM Reporting, a component not available with MOM Workgroup Edition. The four consoles in MOM 2005 and their respective icon representations are illustrated in Figure 3.3 and include on the left-hand side, the MOM Administrator and Operator consoles shown together sharing a single icon. The Administrator console is a Microsoft Management Console (MMC), and is used to manage the setup and configuration of MOM 2005, including global settings, management packs, and agents.

Figure 3.3 MOM 2005 Consoles

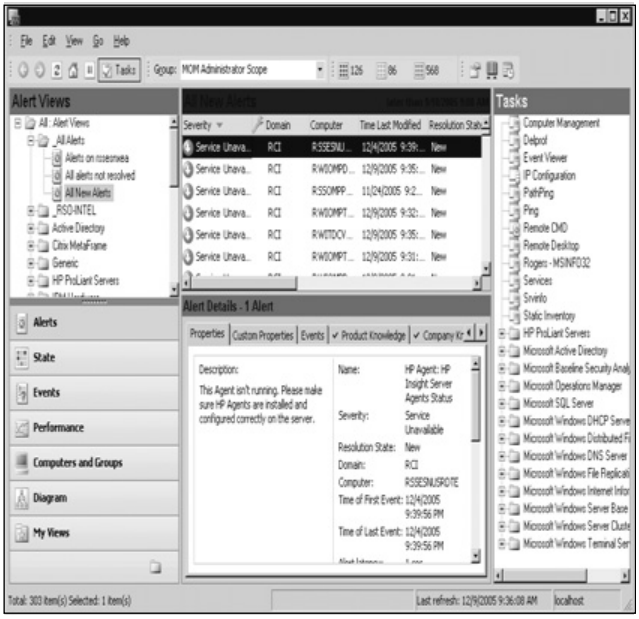


The Operator console is a user interface written in .NET managed code that is designed for your MOM operators to view the events and alerts that are occurring on your monitored systems, and provides an administrative launching pad to take corrective action and resolve the alerts that you are seeing. This resolution activity is accomplished via the Tasks pane in the Operator console shown in Figure 3.4. From an icon perspective, both the Administrator and Operator consoles are represented by a single icon because they are installed together, and you do not have the ability to perform separate and distinct installations of either console. If you are familiar with MOM 2000 but new to MOM 2005 you will notice that the Operator console is a new console that didn't exist in MOM 2000.

NOTE

Because the Operator console is written in .NET managed code, the .NET Framework v 1.1 is required on the system on which you install the Operator console. You can find more information about the .NET framework at http://msdn.microsoft.com/netframework/technologyinfo/default.aspx.

Figure 3.4 Task Pane in the Operator Console



The icon in the middle of Figure 3.3 represents the Web console, and the icon on the right, the Reporting console, both browser-based consoles that provide access into either the operational component of MOM or into the reports. The Web console is an optional component but can prove advantageous in environments where MOM operators are not always sitting at the same system and hence don't always have access to the Operator console. Another work-around to situations like this is to enable Terminal Services in Remote Administration mode on your MOM Management Server and install the Operator and Administrator consoles on the Management Server, allowing you the ability to remotely connect from any system within the enterprise. I am not a huge fan of the Web console myself, because you are much more limited in what you can do than you are with the Operator console, and it requires IIS to be installed. From a security perspective, I always recommend to customers that they try to avoid IIS installations as much as possible since IIS does increase the attack surface on your server. When talking to customers about the features that interest them, I like to probe the clients to learn more about their existing and planned operations management process; specifically, how they plan to work with MOM 2005. What I often find in large organizations is that MOM operators perform 90 percent of their daily work at their desktops, and when they aren't at their desktops, they are at another system with remote desktop capabilities; hence, their likely utilization of the Web console isn't very great at all.

MOM Reporting

An optional component (and I use the word optional lightly) of MOM 2005 is MOM 2005 Reporting. I say this because I have yet to work with or meet a MOM 2005 customer that views reporting as an optional component. But it's not hard to see from the number of reports and time spent developing the reports included with most of Microsoft's Management Packs that Microsoft themselves do view reporting as an optional component, and that's truly unfortunate! From a graphical representation perspective, the three components that make up MOM 2005 Reporting are shown in Figure 3.5, and from left to right include the System Center Reporting data warehouse, System Center Reporting Server running SQL Reporting Services and housing the SQL Reporting Services database, and the SQL Reporting Services console.

Figure 3.5 MOM 2005 Reporting Components

The System Center Reporting data warehouse is used to store data for long-term trend analysis and is the repository or data warehouse that you will query to generate reports. System Center Reporting is built upon SQL Reporting Services, a free add-on to SQL Server 2000. Every evening at 01:00 a scheduled task named SystemCenterDTSPackageTask runs on the MOM Reporting server and transfers to the data warehouse resolved events, alerts and performance information that are set to be groomed from the OnePoint database.

TIP

The default grooming period is set to 395 days for the SystemCenterReporting data warehouse. This default cannot be modified through the GUI interface but can be modified by running the following command in SQL Query Analyzer:

EXEC p_updategroomdays 'TableName', DaystoRetainData

where TableName and DaystoRetainData are the variables. So the next logical question is, what are the tables? The answer to that is SC_SampledNumericDataFact_Table, SC_AlertFact_Table, SC_EventParameterFact_Table, SC_AlertToEventFact_Table, SC_EventFact_Table, and SC_AlertHistoryFact_Table.

Again, as we mentioned previously in our discussion about the Management Server, one or a combination of these roles can exist on a single server. If you have been thinking about hardware requirements as you have been reading through this chapter, it's important to understand that each of the components discussed does not require its own physical server because multiple roles can be configured on a single physical server. That said, don't discount the idea of using multiple servers, because in many environments, that will significantly improve the performance of your solution.

Another important point to stress when we are talking about the different components that make up MOM 2005 is that you do not have to install all these on or around the same time. It's not uncommon for the database and first MOM Management server to be installed, followed by the installation of a core set of Management Packs and some agent deployments. If that is the approach that you do end up taking and MOM Reporting is not installed at or around the same time, you will want to consider the volume of information that will be transferred to the MOM Reporting server when the DTS package runs for the first time.

The DTS job identifies information in your fact and dimension tables in the OnePoint database that has changed since the last time the DTS job ran and prior to a defined latency time. The default latency time is five minutes prior to the start of the DTS job. The latency time can be your trump card when you need to move large amounts of data but want to do it in smaller packages, and it exists to ensure that the records in the OnePoint database are committed across all tables prior to being transferred to ensure data consistency. In the case where you just installed MOM Reporting this will be all data up to five minutes prior to the job first running, but if you have 15 days' worth of data in the OnePoint database it is highly recommended that you move this data in smaller pieces using the /latency switch.

This will shorten the transfer time and prevent the DTS task from failing due to lack of space.

Best Practices from the Field

To use the latency switch, open the Command Prompt on your MOM Reporting server and in the %Program Files\Microsoft System Center Reporting\Reporting directory tree type:

MOM.Datawarehousing.DTSPackageGenerator.exe /silent /srcserver:db /srcdb:OnePoint /dwserver:DW /dwdb: SystemCenterReporting /product:"Microsoft Operations Manager" /latency:12

where 12 is the number of days. This will transfer all data older than 12 days during the transfer. After this task completes, repeat the command using smaller intervals until you have moved all your data.

Now that you are familiar with the various components available in MOM 2005, let's take a look at the four things for which you need to plan.

Planning Basics

When it comes to planning your MOM 2005 architecture, there are four things that you want to plan for:

- Features
- Capacity
- Redundancy
- Configuration

A good place to start, now that you understand the different components available to you, is with the evaluation of the features you want from MOM 2005. From there, take a look at the capacity requirements you have followed by your redundancy requirements and finally, think about how your environment is configured because that will affect how MOM 2005 is deployed.

Let's explore each of these four main planning areas in more detail, starting with a look at features that you want.

Features

When it comes to assessing the features that are important to your organization or your client, start collecting information by asking some basic questions such as:

- What's the timeline for your deployment? Who is going to be responsible for administering MOM 2005 when the deployment is complete? Who is going to be responsible for using MOM to monitor the environment? How many administrators and operators do you plan to have? What is the plan to train these individuals and bring them up to speed on MOM 2005?
- Does your organization use Active Directory? What are the other mission-critical applications that you support in your organization?
- How many offices do you have and where are they located? Are there systems in each of these offices that you wish to monitor? What are the connection speeds between the offices and what does the network topology look like? How does this correlate to AD sites?
- Where are your firewalls located? Do you have systems located behind a firewall that you wish to monitor?
- How many systems do you wish to monitor? Does this include any desktops? If so, what is the breakdown (servers/desktops). What are the operating systems running on these systems? (operating system version and service pack)
- How will your operators/administrators access MOM? Do these people log into the same workstation each day to perform their administration or are they often roaming throughout your organization assisting others with issues? Understanding how these people work will help you to determine whether you really need a Web console.
- Do you need to have people accessing alerts and events over the Internet or through a firewall?
- Does your organization use another monitoring application currently? What is the intended role of MOM 2005 within the organization? Do you need the MCF to hook up to other operations management applications? Is this something that you plan on configuring immediately or is your first phase of the deployment to get MOM 2005 installed, configured, and the rules tuned to reduce the volume of events and alerts to a level that allows for effective administration?

- Do you need reporting? The answer to this question is always yes from my experience but there may be customers out there that feel that reporting is not important to them. A better question around reporting is what type of information are you interested in seeing in a report? This will help you to determine whether the built-in reports will provide that information or whether you will have to create your own custom reports.
- How long do you need to keep the data from your monitoring systems? Break this down into the length of time you need to keep event, alert, and performance data.
- What are you looking to monitor? The answer to this question is usually either "everything" or "what can we monitor?" Narrow this down! Your deployment will be much more successful if you break down the implementation of Management Packs into phases. I generally recommend deploying your core MPs in phase one, which includes the operating system, MOM, DNS, AD, FRS, group policy, Exchange, SQL, and one or more hardware OEM MPs, which will depend on the hardware used within your environment. From there phase two generally includes the ancillary application MPs, which again will depend on your environment and types of applications you support. For organizations that don't have a patch management application, I always recommend the MBSA MP. Phase three focuses on customization, which includes third-party MPs and custom-designed MPs.
- What type of antivirus and antispyware applications do you support? These are prime examples of applications that can be monitored through the creation of custom rules and management packs to allow you to monitor the version of your antivirus definition files and the successful completion of scans as well as failed scans. What backup application do you support? Backup applications, line of business applications, web applications, not to mention hardware and non-Microsoft operating systems, are other excellent candidates for customization.
- Is new hardware going to be purchased or is existing hardware going to be used? If existing hardware is going to be used, what are the specifications of the existing hardware that you have to work with?

Knowing the answers to all these questions during the planning phase will significantly increase the likelihood of success in your MOM 2005 deployment and help you to architect the appropriate solution based on the needs of the organization.

Knowing the features that you want will also help you when it comes time to perform the installation by being prepared for the various prerequisites. For example, the installation of the MOM Management Server requires the .NET Framework version 1.1, MDAC 2.8, and if you want the Web console, IIS with ASP.NET will also be required. The installation of the user interface requires that the .NET Framework version 1.1 and MDAC 2.8, as well as the Operator console, be written in managed code. The database server requires SQL Server 2000 and must have SP3a applied for security reasons. MSDE, although a valid option, isn't a scalable solution for large enterprise deployments and isn't something that can be clustered. The MOM agent can be installed on Windows 2000 Professional or Server with SP3 and later, or Windows XP or Windows Server 2003. And finally, to install MOM 2005 Reporting, SQL 2000 SP3a and SQL Server Reporting Services must be installed.

Understanding these prerequisites is key as these can help you decide if you want to have features such as reporting, which requires an additional SQL Server license, as this may or may not fit into your budget. When it comes to planning and selecting features, the recommended approach is to start simple and design a proof of concept in a lab environment to test the different components and get a feel for the product and its different features, then build upon that base architecture.

Capacity

There are really two dimensions to capacity planning, breadth and depth. Determining the breadth of monitoring you want to do comes down to identifying the number of computers you want to monitor with MOM 2005. You can monitor from one to thousands of servers with MOM 2005, but you have to determine how many servers you are going to monitor within your organization. In a large organization this can be a difficult question to answer initially so break it down into more manageable pieces and start by asking questions like, do you want to manage Exchange? And do you want to manage SQL and Active Directory and then come up with a list of servers that run those enterprise applications, directory services, and other dependent services such as DNS, and FRS?

The second dimension to capacity planning is the depth of monitoring. Do you want to have a lot of rules that are responding to a lot of problems in your environment, or do you want some lightweight monitoring? Do you want to collect lots of performance data for trend analysis and be able to troubleshoot in depth? The question that generally comes out of all these questions is "well how large is the amount of data that will be collected from any one agent?" The best way to answer that question is to attempt to quantify the different types of data that are collected. Table

3.1 provides some detailed numbers that can be of assistance in your database sizing and capacity planning.

Table 3.1 Sizing information

Element	Size
Event	~ 2400 bytes
Alerts	~ 5000 bytes
Performance data	~ 195 bytes

The sizing information in Table 3.1 was provided by Travis Wright, a program manager at Microsoft, during a presentation at the Microsoft Management Summit titled "SM04 Planning and Deploying MOM 2005."

Determining Data Flow

When planning for capacity look at four different types of data:

- Performance Data
- Events
- Alerts
- Attributes/Service Discovery Data

For each of these four different types of data there are two different dimensions: size and volume. Size has to do with the size of the actual data being collected (an average is provided for you in Table 3.1). Here, what's important to understand is that a MOM event is actually much smaller in size than an alert, and performance data is even smaller in size than both an event and an alert. But before you get too excited, look at the amount of data for each of these types that you are going to collect. Throughout the day you are going to collect a much larger number of performance counters on a given server than you are going to receive alerts on a given day, so the volume of performance data collected will be much greater than that of alerts collected. Any time we begin collecting large volumes of information, there is the potential for bottlenecks, which we will discuss later in this chapter, along with how to avoid them.

Looking at the two original capacity dimensions of depth and breadth, you can begin to think about your capacity being like a box, and the larger the box gets, the more complicated your MOM 2005 deployment becomes. This is where understanding the support statement from Microsoft can come in handy in your planning.

Microsoft's official support statement for MOM 2005 SP1 can be found in the MOM 2005 Supported Configuration section under Performance and Scalability at www.microsoft.com/technet/prodtechnol/mom/mom2005/default.mspx. Table 3.2 provides more detailed information on the performance and scalability limits of MOM 2005 SP1.

Table 3.2 Supported MOM 2005 Configurations

MOM 2005 SP1 Feature or Component	Supported Maximum
MOM database size	30 GB
Agent-managed computers per management group	4,000
Agent-managed computers per management server	2,000
Agentless managed computers per management server	10
Agentless managed computers per management group	60
Multitiered MOM management groups	3
Source Management groups reporting to a destination management group	10
Forwarded alerts per day to a destination management group	400,000
MOM consoles per management group	15
Reporting subsystems per MOM database	1
Management servers per multihomed agent	4

Use Microsoft's support information to help you to answer some very simple questions that will help you to determine your high-level architecture. Start by understanding on how many monitored systems you will be installing a MOM 2005 agent, and how will this change over the next one or two years. If this number is under 2000, you can use only a single MOM Management Server. This wouldn't be recommended for redundancy purposes but it's a starting point. This also means that you can start your design with only a single management group. Variables that might suggest that you start your design with multiple management groups include offices in different geographical locations, security requirements, more than 4000 computers to be managed, decentralized administration, and corporate politics being some of the more common.

Having offices in different geographical locations may cause you to lean toward multiple management groups to allow you to isolate the majority of monitoring

traffic within each location, and potentially improve local monitoring performance by having a local OnePoint database. In this type of large, global enterprise deployment monitored agents could be configured to forward some or all of their monitored events, alerts, and performance data to the local MOM Management Server, which would in turn persist that into the local database server. This local management group could then be configured to forward all alerts to a central Management group at your corporate headquarters, allowing alert data to be stored and monitored centrally in your 24/7 network operations center (NOC).

Security requirements may also mandate that more than one configuration group be part of your initial design. Although MOM 2005 was not designed to be a security monitoring and collection application, it certainly can be used in this capacity with the appropriate planning. An excellent third-party management pack is available from Secure Vantage Technologies (www.securevantage.com), which provides you with a wealth of rules and built-in reports to help you quickly and easily begin collecting the information that is of interest to you. It's not uncommon within large organizations to find security handled by a completely independent and often isolated group. If your organization plans to use MOM 2005 to collect security-related information and security is owned by a separate group, this too could be another justification for more than one Management Group as this would provide complete isolation of security data. Normally in situations like this, one Management Group is set up to have all monitored agents send all their monitored data with the exception of security data to this first Management Group, and send only security-related information to the second Management Group, making each agent multihomed. A multihomed agent is simply a monitored computer that reports to more than one and up to four Management Groups. With respect to security, what type of information does the security group want/need collected? Is service monitoring, server uptime, SLA monitoring important to your organization?

Planning on monitoring more than 4000 systems will definitely require you to architect a solution that has more than one Management Group if you plan on staying within Microsoft's support limits, which is always a good idea.

And lastly, decentralized administration may require you to architect a solution with more than one management group to allow the administrators in each department, division, or region to be responsible for their own systems. This requirement is very similar to that discussed in the previous section, which talked about different geographical locations.

Other considerations include which services you are going to monitor. Are you going to be monitoring just Exchange or are you going to be monitoring Exchange and AD? What about DNS, DHCP, File Replication Service, Group Policy, hardware components, not to mention applications like Citrix, Oracle, or line of business

applications? With respect to hardware, what is the underlying hardware platform your organization uses? Are you an HP/Compaq, IBM, or Dell shop, or a combination thereof, and will you be using the various OEM Management Packs? To get a better idea of the different Management Packs that are available, both Microsoft and third-party, look at the MOM MP Catalog at http://www.microsoft.com/mom and identify which MPs you will likely use. Try to break down the MPs that you will use into phases, with phase one including core MPs, phase two including application MPs, and phases three and above including nice-to-have but nonessential MPs.

You will also need to consider what level of monitoring you want to have. Are you interested in a performance counter to help you anticipate growth and plan for your capacity needs? And if so, on which servers, just the Exchange and SQL servers, or all servers?

When MOM 2005 begins collecting large volumes of information, there is the potential for bottlenecks. In the next section we will take a look at what those bottlenecks are and how to avoid them.

Common Bottlenecks

When you take a look at planning for capacity it's important to understand the bottlenecks in MOM 2005. All applications have bottlenecks, and in MOM 2005 the biggest bottleneck is the input and output to and from the MOM database. Very large organizations that are collecting large amounts of events and performance data must make sure they have lots of disk drives in the MOM database server.

The next most common bottleneck is the Management Server MOM Service. As the number of agents you are monitoring increases, the harder the MOM Service (momservice.exe) on the Management Server has to work to keep all that data flowing. This is why the support limit is set at 2,000 monitored agents per Management Server. For best performance you may want to reduce the number of monitored agents per Management Server, and instead of having one Management Server monitoring all those agents, have another Management Server share some of that load.

Another common bottleneck that is outside the scope of MOM 2005 is the network bandwidth between the different components of MOM 2005. A lot of customers have WAN links or satellite connections. For example, one unique implementation of MOM 2005 is the US Coast Guard, which has satellites on each of its boats that upload information over those satellite links, so you can imagine what that throughput is like.

One component that is not a common bottleneck is the MOM agent service that runs on the monitored agent. This service is fully capable of collecting large volumes of data and sending that up to the MOM Management Server.

Improving Performance

So how do we improve performance? There are a number of things you can do to try to improve your overall performance, including:

- Increasing the amount of memory
- Adding more powerful and faster CPUs
- Adding faster disks and increasing the number of disks to improve I/O

You can also increase the size of the disk or change the RAID configuration to improve performance. If you work in a large enterprise you may have SQL Database Administrators (DBAs) that would be more than willing to help you optimize the server configuration for SQL Server 2000 or SQL Server 2005 (pending the support statement from Microsoft, expected in early 2006, stating that SQL Server 2005 will be supported).

TIP

For more information on SQL backend storage best practices and recommendations look to your hardware vendor for hardware configuration options. For example HP has a feature online known as ActiveAnswers where you will find documents such as *Configuring Compaq ProLiant Servers from Microsoft SQL Server 2000, Tuning Compaq ProLiant Server with Microsoft SQL Server 2000*, and *Storage Configuration Guidelines for Database Applications*. These documents can be found at www.compaq.com/activeanswers.

The next thing to consider is improving the network, upgrading the speed of the network or the networking equipment. Then you can take a look at software and evaluate whether you should have Windows 2000 or Windows Server 2003. Windows Server 2003 is obviously the recommended operating system for security, performance, and supportability reasons as Windows 2000 is approaching its end-of-life from a support perspective. The use of a SAN is more of a hardware implementation but this, too, might help to improve performance. I've seen customers where the implementation of a SAN for the MOM Reporting server databases has been

both a benefit and in one case, at least initially a performance bottleneck. What's important to investigate prior to connecting to a SAN is the current performance of the SAN, and the other servers and applications that are currently utilizing it.

Agent Working Set

Customers often are interested in knowing how many resources the MOM agent will use on their production servers. The MOM agent actually uses very few resources to monitor your production servers. Generally speaking, the MOM agent uses about 4 MBs of RAM itself and when you add in the largest Management Pack, the Exchange MP, it jumps to around 12 MBs of RAM, and CPU utilization is always generally less than 2 percent for the MOM processes.

As you are starting to see, planning for capacity is actually a very complex subject, and as such, a lot of larger organizations will actually bring in a consultant to help plan for capacity.

All the information that we have talked about collecting thus far now needs to be analyzed in the context of your organization's specific variables, such as your current network design. With this information you can begin evaluating whether you will be able to support the number of clients you have in your remote sites over specific links based on the link speeds and available bandwidth. And if not, evaluate the other alternatives available to you. One alternative might be to create multiple management groups and have all the agents in the remote site report to a local MOM 2005 management server that uses a database located on a server in the same remote site. The MOM-to-MOM Product Connector could then be utilized to push the alerts from the remote site to the central site where your NOC is located.

So let's take a look at an example of an organization that has 2,000 servers, and run through some preliminary numbers.

- Managed Computers = 2,000
- Alerts/day = 2,000 * 4 = 8,000 bytes
- Data/day = 8,000 * 6,000 = 48,000,000 bytes
- Events/day = 2,000 * 200 = 400,000
- Data/day = 400,000 * 2,500 = 1,000,000,000
- Perf/day = 10,000 * 2,000 = 20,000,000
- Data/day = 20,000,000 * 200 = 4,000,000,000
- Total = 5,048,000,000 bytes ~ 5 GB / day

If your organization has only 300 servers, the number crunching and analysis isn't quite as important, because MOM 2005 is quite capable of handling servers in that volume without any problems, but the complexity definitely increases with the number of monitored agents you add, the number of MPs you plan on deploying, and geographical dispersion.

So, what tools are available to assist you in analyzing all the data you have with respect to your deployment and provide you with some guidance on the right solution to meet your own unique needs? One answer is to look to an organization with expertise in this field, typically any qualified and recommended Microsoft partner. The other option obviously is to perform the analysis yourself. Should you elect to perform the analysis yourself, two tools are available to assist you. These include the MOM 2005 Deployment Planning Worksheet available from Microsoft's Web site and the System Center Capacity Planner 2006 (currently in beta at the time of this writing).

MOM 2005 Deployment Planning Worksheet

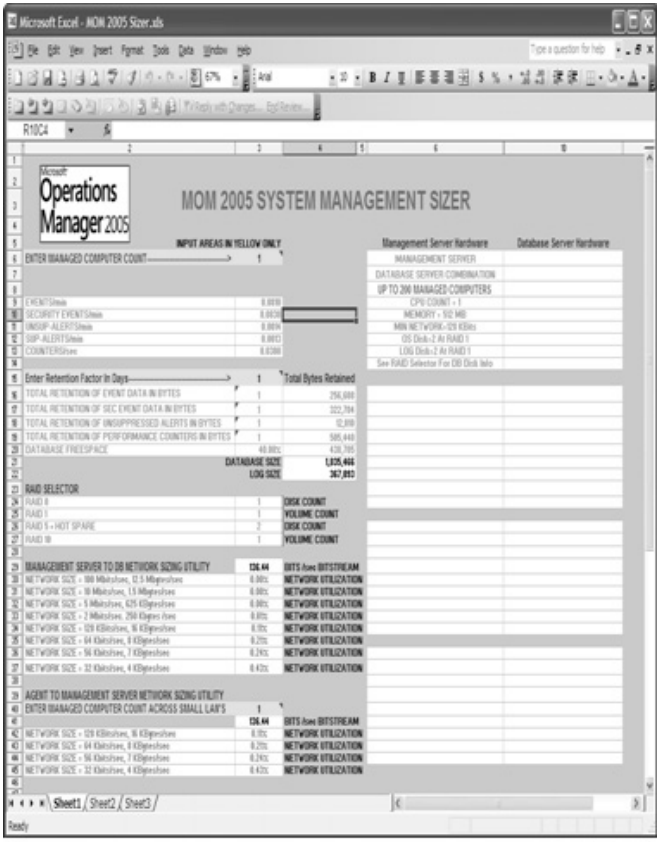
The MOM 2005 Deployment Planning Worksheet is divided into a number of different sections, each designed to help you collect the information required to make an intelligent decision about an appropriate architecture.

The different sections that make up the Deployment Planning Worksheet include:

- Deployment Team
- Software Monitoring Requirements
- Service Level Monitoring Requirements
- Network Environment Considerations
- Organizational Monitoring Requirements
- Failover, Redundancy, and Workload Distribution Scenarios
- Reporting and Reporting Database Requirements
- Upgrade Requirements
- Backup and Restore Requirements

Each of these different sections can assist you in performing a requirements analysis. Once all this information has been identified, collected, and documented, the Microsoft Operations Manager 2005 Performance and Sizing Guide, available on the Microsoft Web site, can be used to help you predict and plan for important performance and sizing metrics for your MOM-specific environment (see Figure 3.6).

Figure 3.6 MOM 2005 Sizer



System Center Capacity Planner 2006

Another application (currently in beta at the time of this writing) is the System Center Capacity Planner 2006. System Center Capacity Planner 2006 is designed to assist with predeployment capacity planning and provide best-practice guidance and hardware-specific knowledge to help you make accurate architecture decisions when planning your MOM 2005 deployment.

System Center Capacity Planner makes it easier for you to perform the following important planning tasks:

- Efficiently plan your MOM 2005 deployment
- Provide system sizing and architecture guidance
- Allow you to perform "What-if" scenarios for hardware, software, and topology

- Increase your confidence in your planned purchases
- Justify the budget required to management
- Meet and exceed performance expectations
- Plan for future needs and business requirements

NOTE

In its current beta version, do not install this on a server running MOM 2005, and be sure to install the Microsoft .NET Framework version 2.0 build 2.0.50215.45 prior to installing System Center Capacity Planner 2006.

Redundancy

MOM 2005 typically is implemented to monitor mission-critical systems such as Exchange and SQL as well as servers playing infrastructure roles such as Domain Controllers, DNS Servers, and Global Catalog servers. Therefore, we want to make sure that not only are these critical services running and fault tolerant, but we also want the application that is monitoring these servers to be redundant; otherwise, we will have no idea what is happening on these servers if the Management Server is not available.

An important question to ask in your planning is how important is redundancy to the organization? In an organization that has a single server running nonmission-critical services, redundancy is usually not a major concern. On the other hand, if the company has hundreds or thousands of servers and the organization depends on services that run on some or all of these servers, then fault tolerance and redundancy becomes something that needs to be considered.

There are three basic ways to improve redundancy, and we will look at each of these:

- Database clustering/RAID
- Agent failover
- Multiple consoles/management servers

From a database perspective, all the databases used in a MOM 2005 implementation can be installed on either a Windows 2000 or Windows Server 2003 cluster.

Using Microsoft SQL Server 2000, you can take advantage of the failover capabilities of the SQL server when installed on a cluster.

The use of hardware RAID arrays is also highly recommended to improve the fault tolerance of the disk drives.

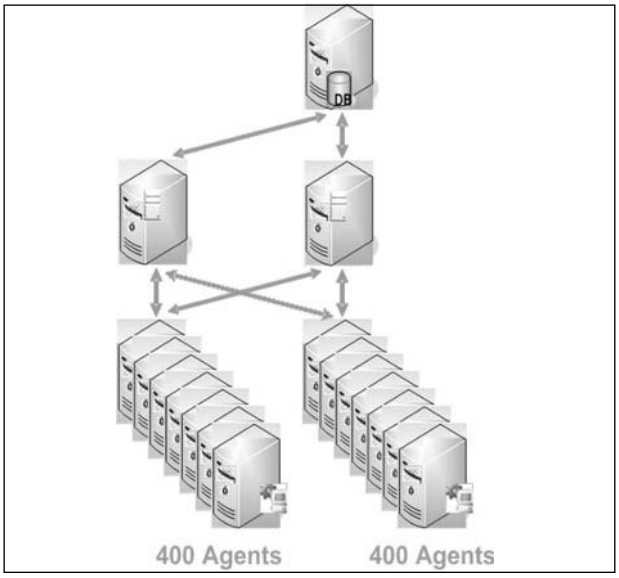
NOTE

MSDE cannot be clustered.

In MOM 2005, in its simplest configuration with only a single management group, each monitored agent is configured to report to a single MOM 2005 management server. Should that single MOM Management Server ever become available during a planned or unplanned outage, the monitored agents will begin to queue up the information they are collecting and store this locally until communication is restored. Both the MOM Management Server and the MOM agent have a configurable storage buffer set through the Administrator console in Global Settings.

To avoid this type of unavailability, it is recommended that a second MOM Management Server be installed in the configuration group and the monitored agents load balanced between the two Management Servers. If we use the example of an organization with 800 monitored agents, this would require a single MOM database server and two MOM Management Servers. This type of design could be configured to have 400 agents report to the first MOM Management Server and the other 400 agents report to the second MOM Management Server, thereby balancing the load and offering redundancy at the Management Server level as shown in Figure 3.7.

Figure 3.7 Simple Management Group Configuration



In this type of configuration, where each MOM 2005 Management Server is monitoring 400 agents, if you need to apply a patch or service pack or perform scheduled maintenance on one of the MOM Management Servers, the 400 agents configured with that Management Server as their primary Management Server will automatically fail over to the other MOM Management Server. The monitored agents will also continue to query their original primary Management Server for availability, and once their primary Management Server becomes available again they will automatically fail back over to it. At this time, the MOM Management Servers are not cluster aware and cannot be installed on a cluster for failover unlike the SQL 2000 application used by the MOM database.

So when it comes to planning for Management Server failover it is important to keep Microsoft's support limits in mind and ensure that the total number of agents reporting to a single Management Server will remain below the supported limit, especially in a failover situation.

If redundancy is important to your organization, you can start by adding multiple servers. This will allow agents to report to another MOM 2005 Management Server if one of the servers should go down. Without the second server, data collection will not be available, which will result in you being blind to what is going on in your environment.

Another important consideration is having multiple consoles installed to see what is going on. If you have only one console installed and the computer that has

the console goes down for some reason, you will not be able to see the status of your environment.

You could also consider using some type of network load balancing or Virtual IP technology for the Web console and install the Web console on multiple servers so that if one of the servers fails you are still able to connect using the Web user interface.

Configuration

Environments are getting more and more complex every day. With installations of firewalls, VPNs, WAN links, and other technologies, we must consider how these different issues will affect our MOM 2005 deployment.

We must consider several factors when looking at the deployment, including:

- Network
- Remote sites
- Firewalls
- Connection speeds
- Business Groups
- Monitoring Groups
- Locale/Language

When considering how the network will affect your deployment of MOM 2005, you will have to consider the number of agents in your remote sites and the placement of the MOM 2005 Management Servers.

A good rule of thumb is that if you have fewer than 25 agents you may want to consider having a single central Management Server. With more than 25 agents but less than 1,000, consider having a Management Server locally (in the remote site) to the agents. If fault tolerance is a concern, then add a second Management Server. Once you surpass 1,000 agents, consider creating a new management group.

Remote Sites with Fewer Than 25 Agents

Here is a scenario where the remote sites have less than 25 agents each. All the remote agents send the data across the Internet to a central site that contains the Management Server and the MOM 2005 database.

Remote Sites with More Than 25 Agents but Fewer Than 1,000 Agents

In this scenario, the Management Server will be located in the remote site where the agents reside. The MOM database is still located in the central site. This allows the agents to communicate locally to the MOM 2005 Management Server where the data is queued up and forwarded to the MOM database in the central site.

Remote Sites with More Than 1,000 Agents

When you have sites with thousands of agents, you may want to consider a tiered architecture in MOM 2005 with one or more child management groups forwarding information up to a single parent management group. In this type of architecture, each of the remote sites will have its own MOM 2005 management group.

In this scenario, each of the sites are self-contained, with every site having a MOM 2005 Management Server, MOM database, and monitored agents. The monitored agents send data to the local MOM 2005 server and the data is stored in the local database. The next step in this type of configuration is to use the Microsoft Connector Framework (MCF) and the MOM-to-MOM Product Connector (MMPC) to send the alerts and service discovery data to the central site where the parent tier resides. This allows you to monitor the entire enterprise and see all the alerts and service discovery data collected throughout the enterprise in a database at the central site.

Firewalls

As we become more and more aware of security issues, firewalls are becoming more prevalent in our environments. Firewalls will introduce challenges into your design and force you to consider a number of additional configuration issues.

HTTP connectivity such as the Web console (to Web server), reporting console (to reporting server), agent (to file transfer server), and MCF are all supported through firewalls. This communication is the same as any other http connectivity, and therefore, we must have TCP port 80 open. Microsoft does recommend and encourage you to open TCP port 443 and use SSL to encrypt the communication to increase security.

Agent managed computers can also communicate through a firewall with the Management Server using the MOM proprietary channel on TCP / UDP ports 1270. This too is a secure communication solution that uses windows encryption. One important piece to note in this type of configuration, however, is that even though a monitored agent can communicate with the Management Server through

the firewall, the agent itself must be installed manually. This is discussed in more detail later in this chapter.

Support for the Management Server communication to the backend database is also available. This is done using OLE DB tunneling, and there are several places on the Internet to find information regarding this strategy. Ports that must be open include the defaults for SQL Server, TCP 1433, UDP 1434.

The Administrator/Operator console and Management Server use DCOM to communicate, which presents a problem when going through a firewall. The problem is that the ports used are assigned dynamically, and therefore a large number of ports would have to be opened at the firewall. Although this can be done using DCOM port binding, it is not recommended, nor is it a supported configuration.

The last consideration is the managing of agentless systems, which is not possible through a firewall. Agentless monitoring uses RPC to communicate with the Management Server, and RPC through firewalls is not supported.

When working in environments where firewalls exist between agents and the MOM 2005 Management Server or between the MOM 2005 Management Server and the database, remember to open the following ports and make the following configuration changes:

- For HTTP, open port 80 on the firewall or use SSL for encryption/authentication and open port 443.
- For OLE DB, open ports 1433, 1434 on the firewall.
- For DCOM, try to avoid using this through the firewall, but if that isn't possible, use DCOM port binding, turn off network address translation (NAT), and open port 135 on the firewall. More information on these configuration settings can be found in the whitepaper "Using DCOM with Firewalls" (http://www.microsoft.com/com/wpaper/dcomfw.asp).
- For the MOM channel and communications between the agents and the MOM 2005 Management Server, open port 1270 on the firewall.

When planning your deployment, keep in mind the following factors with respect to network line speeds. To determine the placement of the Management Servers (central site or remote site), you must consider three main factors:

1. How many agents are there per site?
2. How many sites are there?
3. What are the line speeds between the sites?

Some general rules of thumb include:

- If the number of sites is greater than 10, use a central Management Server. This is because only 10 Management Servers are supported in a single management group.
- When you have a large number of agents per site, the recommended configuration is to place one or more Management Servers in each remote site.

Some additional network speed planning best practices include:

- Always put the MOM database and System Center Data Warehouse on a fast connection (greater than 10 Mbps).
- Put your Administrator and Operator consoles on a fast connection to the Management Servers.

Business/Monitoring/Language Considerations

When looking at your business, your organization may have business units that would like to perform their own monitoring. You may have business groups that are located in different geographical locations, with different language requirements. The organization might also have more than one IT monitoring group, such as an IT security group and an application server administration group. Each of these groups may want its own MOM server to manage its particular line of business.

Based on these possible requirements you will have to consider these factors when designing the architecture. Some alternatives include:

- Create a Management Group for each business unit.
- Create a separate Management Group for the security team—use multi-homed agents.
- Create a Management Group for English and one for German.

Manual Agent Installations in Environments with Firewalls

One of the considerations in an environment with firewalls is how to install the agents, since the automated agent installation option will succeed only on agents residing inside a firewall. Once installed, agents can communicate through a firewall, but the issue is that automated installation across a firewall will fail because the remote installation requires RPC and SMB connectivity, and these ports are generally closed for obvious security reasons.

Therefore, the agents will have to be installed manually. Once the agent has been installed then the communication will occur over the MOM secure channel using port 1270, so it is important to ensure that this port is open before you begin your client installations.

With MOM 2005, the agent installation has been packaged in a Windows Installer file named MOMagent.msi. This file can simply be copied to the agent computer and then run locally, assuming you have the appropriate permissions to execute this installation. On the MOM 2005 Management Server, it is important that you first turn off the Reject Manual Agent Installs option in the global settings, prior to installing the agents, otherwise the agent will not be able to communicate with the MOM 2005 Management Server. This option is a new security feature that has been added to MOM 2005 to prevent rogue agents from connecting to the Management Group and potentially causing a denial of service attack against the MOM 2005 Management Server and database.

The other alternative method (but not recommended) if you have a large number of agents that must be installed through a firewall, is to temporarily take down the firewall and install all the agents remotely. The obvious problem with this strategy is security, and therefore it should be considered only as an absolute last resort. A better solution is to use a tool like Systems Management Server (SMS) to push the software out to the computers or script the installation using msiexec.exe and VBScript or JScript.

Network Speeds

Another consideration in agent deployments is the existing line speeds in your network. Network speeds can have an impact on the configuration of MOM 2005. While considering the network speeds, think about what communications will impact the network traffic the most.

Most of the traffic that is of concern is directly related to the database. The communication between the MOM 2005 Management Server and the database is constantly active with data transfer. This requires fast network links to get the best performance. Another issue related to the database is the bulk transfer of data between the MOM database and the System Center Data Warehouse. This transfer uses the DTS service to move large amounts of data in a single process. When the DTS package runs, you see a large network utilization spike between the computers involved.

Anyone who has ever done remote administration of any kind knows that waiting for feedback from the computer after executing a command is frustrating. Therefore, make sure the operator experience will be enhanced by using fast net-

work connections between the Management Server and the system with the operator consoles.

Some traffic is of less of a concern because it doesn't generate as much volume. Examples of this are Agent to Management Server, Web console, and reporting console traffic.

Planning for Users

Another issue to take into account is the type of access that you will need to provide to your MOM operators and administrators. MOM 2005 offers the flexibility required to meet the needs of all support operations staff by focusing on two usability scenarios: discovery and automation.

The user interfaces make it easy for a user to discover where to start a task, or where to go in the user interface to change a configuration and guide a user unfamiliar with the interface through the completion of the task using wizards and dialogs. Examples of discoverable entry points include the Install/Uninstall Agents Wizard, which automates the process of installing and uninstalling agents, and the Import/Export Management Pack Wizard, which automates the importing or exporting of an MP.

The interfaces are both role-based and task-based, and map to a set of local groups that are created when MOM 2005 is installed. These groups include:

- MOM Administrators
- MOM Authors
- MOM Service
- MOM Users
- SC DW DTS
- SC DW Reader

Table 3.3 summarizes the local groups created during the installation of MOM 2005, and describes their purpose.

Table 3.3 MOM Local Groups

Group	Description
MOM Administrators	Members have full access to the MOM feature set, including all the installed MOM consoles allowing them to view and modify settings and make configuration changes.
MOM Authors	Members have full access to the Operator console and have limited access to elements in the Administrator console. They can view and change settings in the Operations and Management Packs nodes in the Administrator console and view and modify settings in the Operations console.
MOM Service	This group is intended to be used by MOM services and processes and should not contain individuals as members. When separate DAS and Action Accounts are used during the installation, only the DAS account should be a member of this group.
MOM Users	Members can view and modify settings in the Operator console and in the Operations node of the Administrator console.
SC DW DTS	This local group is created on both the MOM database server and the MOM Reporting server and its members can transfer operational data from the MOM database to the MOM Reporting database. Members of this group can view the MOM database and view and modify information in the MOM Reporting database.
SC DW Reader	This local group is created on the MOM Reporting server and members of this group can view information in the Reporting Database.

Proper planning of your local group memberships will allow you the ability to provide access to the different areas within each of the MOM 2005 consoles and provide you with the ability to delegate tasks. Now that you are familiar with the local groups that are created during the installation, let's spend a few minutes reviewing the accounts that you will be prompted for during the installation.

TIP

Remember when planning accounts that members of the local Administrators group on your Management Servers will be able to perform all MOM operations as if they were members of the MOM Administrators group.

MOM Accounts

In MOM 2005 the MOM Service runs as Local System when MOM is installed on either Windows 2000 or Windows Server 2003. Thanks to the security improvements made in Windows Server 2003, you have the option of running the MOM Service as Network Service for increased security. This allows the MOM Service to function with lower privileges. The primary role of the MOM Service is to manage communications between the agent and the MOM Management Server and to run the MOM agent on the Management Server as a monitored computer.

NOTE

Workgroup Edition: The DAS account can be run as Local Service in the MOM 2005 Workgroup Edition.

Windows Server 2003 includes a new built-in account known as the Network Service (NT AUTHORITY\NetworkService) account. This account is a predefined local account that can be used to start a service and provide the security context for that service. The Network Service account has limited access to the local computer and authenticated access as the computer account to network resources. The benefit of using the Network Service account rather than a local or domain user account for the DAS security context is that it will operate with lower privileges and avoid password expirations that may be an issue with domain accounts.

Best Practices According to Microsoft

- Microsoft does not support the changing of the credentials under which the MOM Service runs because this can result in communication failures with agents and lead to other problems in your MOM environment.
- The MOM Service will not start unless it is running as either Local System or Network Service.

During the installation of MOM 2005 you will be asked to provide credentials for two accounts and given the option to use the same credentials for both accounts. These two accounts are referred to as the Data Access Server (DAS) account and the MOM Action account.

DAS Account

The function of the DAS Account is to provide a security context for communication between the MOM Management Server and the MOM database. The DAS account is also used by the MOM-to-MOM Product Connector (MMPC) to facilitate authenticated communication between the MOM database server in a child management group and a MOM database server in a parent Management Group.

The DAS Account now requires fewer privileges when installing a clean installation of MOM 2005 than it did in previous MOM versions. If you upgrade from a MOM 2000 SP1 Configuration group to a MOM 2005 Management group, the settings and permissions for the DAS Account are left unchanged and higher than is necessary for its operation. These settings can be changed after the upgrade to lower the privilege level for the DAS Account.

Action Account

The Action Account is new in MOM 2005 and is used to gather operations data and to run responses and scripts on the monitored computers, including the agent on the Management Server. The Action Account is a separate account in MOM 2005, allowing you to separate the MOM Service context and the response context on monitored systems, including the agent on the Management Server.

The Action Account on the Management Server can also be used to install, uninstall, or update settings on agents on remote computers. This activity requires that the Action Account be a member of the local Administrators group, which is most easily accomplished by adding the Action Account to the Domain Administrators group, though this is not always permitted in all organizations.

Fortunately, the Action Account does not need to be a member of the Domain Admins group as you have the option in the Agent Install/Uninstall Wizard to specify alternate credentials allowing you to specify Domain Admin credentials for the initial installation and then have the Action Account run as a normal user account.

Shortcuts…

The Action Account

The Action Account in theory can be configured to operate in the security context of a low privilege user account; however, in reality, this will be dependent on the MPs you wish to incorporate into your operations management infrastructure since certain MPs do require that the action account either have local administrative permissions or run as local system. One example of this is IIS. In order to monitor the Internet Information Services (IIS) logs, the action account used by the MOM agent on the system running IIS cannot be a low privilege account. IIS as an operating system component can be configured to write operational information to a log file over the course of a day, after which time the log file is saved with a date stamp for that day and can subsequently be viewed. A new log file is then created for the following day. With MOM, the MOM agent is able to read this information as it is being written to the log file and monitor for specific entries, allowing you to be alerted based on real-time events.

Even cooler than that is the new Web Sites and Services MP, which allows you to create and run synthetic transactions against your Web site to validate functionality on an ongoing basis.

Security Requirements

The topic of planning wouldn't be complete without a discussion about security in your MOM 2005 deployment. A security evaluation should start with an evaluation of the potential risks, and a prioritization of those risks within your organization. Next an analysis can be performed to assess each of the risks and determine the available alternatives.

Reducing your security risks in MOM 2005 really boils down to evaluating the need for the following configurations:

- Enable mutual authentication, SMB signing, or IPSec to prevent against man-in-the-middle attacks.
- Use a local account or an account with reduced privileges for the agent Action Account to prevent an attacker from using this account to compromise your network if they can guess or obtain the password.
- Secure communications between the Management Server and the Web console and between the Reporting Server and Reporting console by using SSL encryption or IPSec.
- Secure traffic between MCF connectors by using SSL encryption.

Your ongoing operational security plan should include a regular review of the MOM security group membership to ensure that there are not any unauthorized members being added to the higher privileged group and that the membership of the MOM Service group remains consistent. A regular review of the SQL logons is used by MOM to confirm that only authorized users are included in this logon and that the database System Administrator (SA) role is configured per your security standard. MOM can be used to help facilitate the monitoring of security by collecting specific events from the Windows Security log, including logon events. Be careful in your implementation of security monitoring, however, and watch the growth of your OnePoint database carefully after enabling any new rules. Security rules tend to collect a very large amount of data and if improperly configured can bring your entire MOM infrastructure to its knees.

Best Practices According to Microsoft

- If you decide to use MOM to collect security related information, implement this in a staged approach and use caution when enabling and testing new rules.
- Microsoft recommends that you archive security events often and set the grooming settings to groom more aggressively on your OnePoint database.

Managing MOM Accounts

Another common security requirement that is very likely to present itself in every organization is the need to change the password of the different accounts used in the configuration of a MOM infrastructure.

MOM Action Account

Due to the requirement for the MOM action account to be a domain account in order to access Active Directory, it is very likely that password policy will require that its password expire or be changed on a regular basis. After changing the account's password in Active Directory, the SetActionAccount utility found in %Program Files%\Microsoft Operations Manager 2005 can be used to change the password of this account on the Management Servers. Following the change, the MOM Service must be restarted. This is true of any permission change to the Action Account.

The syntax to change the password is **setactionaccount.exe Mgmt1 -set contoso momaction**, where **Mgmt1** is the name of the Management group and **momaction** is the name of the Action Account in the **contoso** domain. When you execute this command you will be prompted for the password and then again to confirm the password. You will also be notified whether the account you specified is a member of the Domain Administrators group. Don't forget to restart the MOM Service on the Management Server(s) after you change the password.

MOM DAS Account

After changing the password for the DAS account in Active Directory, update the password on the Identity tab in the properties of the Microsoft Operations Manager Data Access Server COM+ application. This can be found in the Component Services snap-in. After changing the password, stop and restart the COM+ application.

Best Practices According to Microsoft

- If you are changing the Management Server Action Account and the DAS account at the same time, be sure to change the Action Account first, followed by the DAS account. Then restart the MOM Service on the Management Servers before stopping the COM+ application. Starting the MOM Service will also start the COM+ application.
- If the MOM service will not start, confirm that the DAS account has been changed correctly and that the password hasn't expired.

You can also change the account MOM uses for the Data Access Service (DAS) functionality, but the account must be a domain account and must have the following properties:

- Member of the MOM Users group on the Management Server
- A SQL Server Logon with "Permit" server access and "db_owner" (DBO) access to the OnePoint database on the MOM Database Server
- Member of the SC DW DTS security group on the MOM Reporting Server and MOM Database Server, if MMPC is installed using the DAS account

Disaster Recovery Planning

The topic of disaster recovery planning is a book in and of itself so the focus of this section will be on the key disaster recovery planning (DRP) issues that you should be planning for with MOM 2005. The key to recovery in MOM is the MOM database, because this is the repository for all of your MOM configuration data. Regularly backing up the OnePoint database is critical to being able to successfully restore your MOM configuration. In addition to backing up the database, it is also a good idea to back up your MOM Management Servers though in a worst-case scenario, these systems could be rebuilt with the same name and configuration as they had before the disaster.

Another good practice to following is to regularly export your management packs and save these to a location on the network so that if you ever accidentally overwrite a set of custom rules with an update to an existing MP you can quickly restore your previous configuration.

TIP

A quick and dirty batch file can be used to help you automate the backup process using a built-in utility known as ManagementModuleUtil. Simply create a batch file with the following line in it and duplicate the line for each installed MP:

"c:\Program Files\Microsoft Operations Manager 2005\ManagementModuleUtil.exe" -O *MgmtServer* "Microsoft Identity Integration Server" "d:\MPExports\Microsoft Identity Integration Server.akm" –W

Replace *MgmtServer* with the name of your Management Server and change the name of the MP as well as the name you wish to save it as, and schedule it to run daily at a convenient time.

Advanced Configurations

There are number of topics that fall within the category of Advanced Configurations, but in this section we are going to limit our coverage to include only a brief overview of the five MOM 2005 Solution Accelerators.

MOM 2005 Solution Accelerators

The five MOM 2005 Solution Accelerators are designed to provide technical and prescriptive guidance and help organizations reduce the cost of operations. The Solution Accelerators can be downloaded for free from http://www.microsoft.com/mom/evaluation/solutions/default.mspx, and include:

- Notification Workflow
- Autoticketing
- Alert Tuning
- Service Continuity
- Multiple Management Group Rollup

The Notification Workflow Solution Accelerator provides guidance on how to use a Microsoft SQL Server Notification Services application to extend the notification functionalities of MOM 2005.

The Autoticketing Solution Accelerator provides guidance on how to automate ticket generation and enable the automated posting of a ticket into a Trouble Ticketing (TT) system that is used for incident management.

The Alert Tuning Solution Accelerator provides guidance on how to identify the most common alerts and reduce the volume of these and other alerts.

The Service Continuity Solution Accelerator provides guidance on maintaining the availability of MOM 2005.

The Multiple Management Group Rollup Solution Accelerator provides guidance on how to propagate data from multiple management groups into one data warehouse to allow for the creation of consolidated and aggregated reports.

Summary

There are many facets to the planning of a MOM 2005 architecture and the complexity of your design will be based on the needs of the organization and their monitoring goals. In this chapter you have learned about the different components that can make up your MOM 2005 architecture and have looked at a number of different areas involved in the planning of your MOM topology including capacity, redundancy, and configuration planning. You have also learned the questions to ask to assist you in planning your administrative delegations and security requirements, and looked at the key components of a MOM 2005 disaster recovery plan. We wrapped up this chapter with a look at the MOM 2005 Solution Accelerators and provided a brief overview of what each of these can offer you and where to find them when faced with more advanced configurations.

Planning your MOM 2005 infrastructure is not difficult but does require that you perform your due diligence and collect the information required to allow you to make the required decisions. As you start your collection, analysis, and planning, keep the four main planning areas in mind: features, capacity, redundancy, and configuration. Take advantage of the tools and documentation available to you in the form of the capacity planning worksheets, performance and sizing whitepaper, and the new System Center Capacity Planner utility. Remember that planning is time well spent.

Solutions Fast Track

Planning Your MOM Topology

- ☑ A management group is made up of a single MOM database, one or more MOM Management Servers, and one or more monitored agents.
- ☑ A more complex MOM architecture can have a child management group configured to forward operational data to a parent management group.
- ☑ Up to 10 child management groups can report to a single parent management group.

Planning for Features and Configurations

- ☑ Planning in MOM 2005 can be broken down into four main areas including planning for features, capacity, redundancy, and configuration.

- ☑ Planning for features involves identifying which features you want.
- ☑ Capacity planning involves determining the amount of information you plan on collecting, the number of agents you want to deploy, the number of MPs you want to install, and the configuration of your network.
- ☑ Redundancy planning involves looking at the availability needs of your monitoring infrastructure.
- ☑ Configuration planning will take into account security requirements, delegated administration requirements, and geographical locations, as well as available network bandwidth.

Planning for Users

- ☑ MOM 2005 creates a number of local groups that can be used to provide delegated administration.
- ☑ Console scopes can be used to limit what is seen in the Operator console and what changes a user is able to make.
- ☑ MOM Reporting uses SQL 2000 Reporting Services, which can also be configured to provide different levels of access to your reporting infrastructure.

Security Requirements

- ☑ During the installation of MOM 2005 you will be asked for the credentials of two accounts, the DAS Account and the Action Account. The DAS Account requires fewer permissions in MOM 2005. It no longer must be a member of the local administrators group on the database server but does require db_owner rights on the OnePoint database.
- ☑ Multiple management groups provide increased security through the physical separation of specific data into different databases.
- ☑ Command lines are now explicitly separated into Program and Arguments to prevent execution of trojans.
- ☑ Task execution auditing allows you to quickly identify what task was run, when, by whom, against which computers, and whether it was successful.
- ☑ Most scenarios will not require agent proxying, however the Active Directory Management Pack does if you elect to use the Client Side

Monitoring rules, as does the Exchange MP on at least one Exchange Server in order to utilize topology discovery. Proxy-enabled agents can communicate on behalf of any managed device.

- ☑ Manual agent installations are rejected by default to prevent rogue agents from connecting to your MOM 2005 management group.

Disaster Recovery Planning

- ☑ Backing up your OnePoint database is the key to disaster recovery planning in MOM 2005.

Advanced Configurations

- ☑ The five MOM 2005 Solution Accelerators provide technical and prescriptive guidance on how to plan and implement more advanced configurations.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: What are the four main planning areas to focus on when planning a MOM 2005 architecture?

A: When planning for MOM 2005, decide upon the features you want, look at your capacity requirements, evaluate the availability requirements of your operations management application, and then think about your configuration options.

Q: Are there any dependencies for the installation of the different MOM 2005 components?

A: Yes, the database must be installed first, followed by a Management Server. From there you have some options as to what is installed next, including

MOM reporting. MOM agents can be deployed or Management Packs can be installed.

Q: What types of design requirements will require that more than one management group be created?

A: Normally geographical dispersion and security are the two driving factors behind multiple management groups. Politics can also play a role in this decision.

Q: What is the MOM Host (Action Account) used for?

A: The Action Account is used to collect data on a monitored agent and is also the security context in which a response is executed. The action account also is used for discovery and agent management on the Management Server. This account requires administrative level rights on Windows 2000 and Windows XP but not on Windows Server 2003.

Q: In what context does the MOM Service Account run?

A: The MOM Service Account runs as LocalSystem by default on Windows 2000 and Windows XP, but can be configured to run as Network Service on Windows Server 2003.

Q: What are the minimum privileges required for trusted monitoring by the Action Account?

A: The Action Account must be a member of the local Users and Performance Monitor Users groups, and must be granted the Manage auditing and security log (SeSecurityPrivilege) and Allow logon locally (SeInteractiveLogonRight) rights. These are the absolute lowest privileges that MOM 2005 supports, but in reality, your actual permissions and privileges will depend on the Management Packs that you are deploying and supporting. For example with the SQL MP, using a low-privilege account will require that you make numerous configuration changes to get things to work as expected. Because there will be limitations with some scripts, SNMP notifications will not work nor will NIC monitoring, so in using a low-privilege account, you do make some sacrifices. Also keep in mind that the use of a low-privilege account is available only when running MOM 2005 on Windows Server 2003. When running MOM 2005 on Windows 2000

Server, the action account must be a member of the local administrator security group.

Q: What local group must I be a member of on the MOM 2005 Management Server in order to launch runtime tasks?

A: To launch runtime tasks, you must be a member of either the MOM Authors or MOM Administrators local groups. Remember that there are two types of tasks available in the MOM operator console: console tasks and runtime tasks. Members of the MOM Users group are able to execute only console tasks for the scope that they belong to.

Chapter 4

Installing Microsoft MOM 2005

Solutions in this chapter:

- **Installing on a Single MOM Server**
- **Installing on Multiple MOM Servers**
- **Upgrading to MOM 2005**
- **Advanced Scenarios**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

Installing Microsoft Operations Manager 2005 is not as simple as it might sound. Depending on what version of the software you are installing and the type of installation you are performing, the prerequisites for your installation will vary and the effort you will need to put into the installation will determine how well the installation performs later. There are three basic types of installations that you will need to consider, and each type of installation has its own requirements. This chapter is meant to walk you through the various pitfalls that might confront you as you perform your MOM 2005 installation.

Installing on a Single MOM Server

As with any software application installation, one of the first steps in preparing to install Microsoft Operations Manager on a single machine is to verify the computer chosen to host the installation meets the minimum hardware and software requirements. In Chapter 3, you determined what your objectives for your installation of MOM 2005 would be. What those objectives are will determine how you will use MOM and that determines what components need to be installed.

Shortcuts...

Getting Started

Even though you carefully planned your objectives for the installation of MOM 2005 in Chapter 3, there are a few things you should go over one more time before you begin the installation. Those things you should review include:

- MOM 2005 Key Concepts
- Your deployment design and planning documents developed in Chapter 3
- MOM 2005 release notes to identify any changes in the software that could affect your original plan
- The MOM 2005 Performance and Sizing Guide
- The MOM 2005 Security Guide
- The MOM 2005 Supported Configurations data sheet

It's best to go over these items now before you begin your installation so that any potential difficulties may be overcome at this point in time.

Depending on what components you want to install, the minimum hardware and software requirements vary slightly. The MOM Prerequisite Checker in the MOM Setup shown in Figure 4.1 should be used to verify the hardware and software prerequisites and to create a report listing those requirements that your installation destination meets or fails to meet. Complete information concerning hardware and software requirements can be found in the MOM 2005 Supported Configurations data sheet that is located on the MOM 2005 installation CD.

Figure 4.1 Check the Prerequisites before Installing MOM to Verify the Hardware and Software Installations

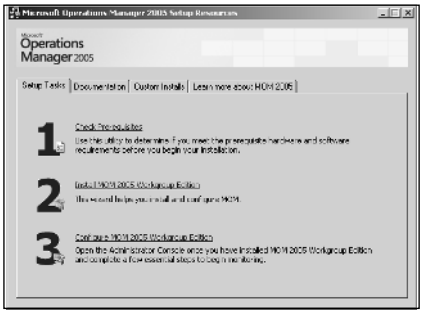
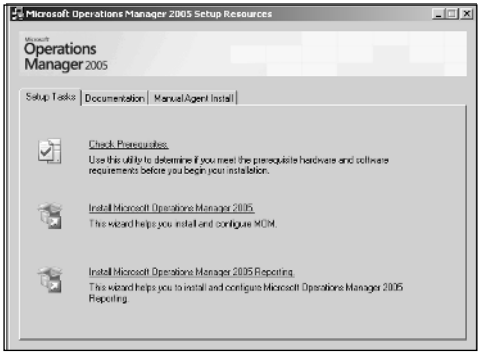


Figure 4.1 illustrates the Setup Tasks tab of the MOM 2005 Setup Resources Window for MOM 2005 Workgroup Edition. Figure 4.2 illustrates the same tab from the MOM 2005 Setup Resources Window for MOM 2005.

Figure 4.2 The MOM 2005 Setup Resources Window from the MOM 2005 Evaluation Edition



Whichever version you are installing, the basic premise is the same and running the MOM Prerequisite Checker is simple. As seen in both Figure 4.1 and Figure 4.2, the MOM Prerequisite Checker is the first option in the MOM 2005 Setup

Resources window that appears when you put the MOM 2005 CD in the target computer's CD-ROM unit. Depending on which version of MOM 2005 you are installing, clicking Check Prerequisites will either bring up the Check Prerequisites dialog window as seen in Figure 4.3 from the MOM 2005 Workgroup Edition, or that seen in Figure 4.4 from MOM 2005.

Figure 4.3 Choose the Complete Option to Check the Prerequisites for All MOM Components

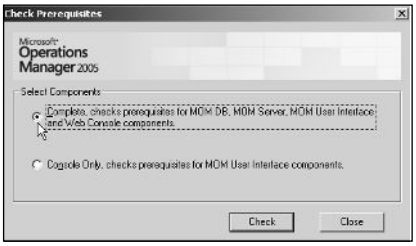
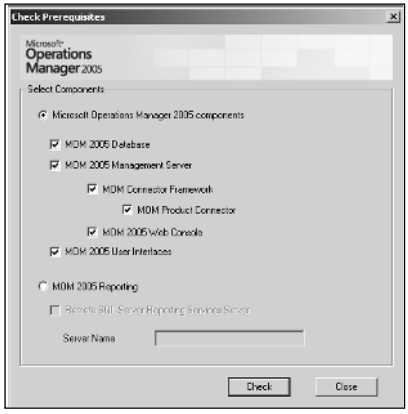


Figure 4.4 The Two Versions Show Considerable Difference at This Point



The Workgroup Edition allows you simply to check an option and it checks all prerequisites for you. The Standard version allows you to specify which options you wish to check and which you wish to ignore. Whichever option you choose, simply either click the **Complete** option in the Workgroup Edition or check the options you wish checked in the Evaluation Edition and then click the **Check** button. In a few short minutes both versions will produce a report that will open in Internet Explorer and provide a list of the prerequisites and their status on the target host. This is a very important document and you should print it out and refer to it again as you make adjustments to the computer's hardware and software in an effort to meet the requirements for MOM 2005. You will probably want to run the MOM Prerequisite Checker two or three times more as you bring the system into compliance.

The installation of the various versions of MOM 2005 that you might decide to install will all be very similar as can be seen in the figures. During the various installation scenarios discussed in this chapter, both versions will be shown when there is a major difference.

For our first example scenario, all the MOM components are going to be installed on a single computer. If you need to manage less than 200 computers, all the MOM 2005 components can be installed on a single computer with little problem as long as the potential host system meets the following hardware requirements:

- A Pentium-compatible 550MHz dual-processor or better
- A minimum of 1 GB of RAM (4 GB or higher recommended)
- 1 GB of available hard drive space (more space might be needed for Reporting)
- A CD-ROM
- A network card

Because this scenario requires the installation of all necessary components on a single MOM server, the installation will have specific software requirements. The minimum operating system on our proposed host to meet this single host requirement will need to be Windows 2000 Server with Service Pack 4 or later. Other operating system options include:

- Windows 2000 Advanced Server with Service Pack 4 or later
- Windows 2000 Datacenter Server with Service Pack 4 or later
- Windows Server 2003 , Standard Edition
- Windows Server 2003, Enterprise Edition
- Windows Server 2003, Datacenter Edition
- Windows Server 2003, Web Edition
- Windows Server 2003 , Standard Edition with Service Pack 1
- Windows Server 2003, Enterprise Edition with Service Pack 1
- Windows Server 2003, Datacenter Edition with Service Pack 1
- Windows Server 2003, Web Edition with Service Pack 1
- Small Business Server 2003
- The 64-bit version of Windows Server 2003, Standard Edition for 64-bit Itanium-based systems

- The 64-bit version of Windows Server 2003, Enterprise Edition for 64-bit Itanium-based systems
- The 64-bit version of Windows Server 2003, Datacenter Edition for 64-bit Itanium-based systems
- The 64-bit version of Windows Server 2003, Web Edition for 64-bit Itanium-based systems

In addition to the operating system, there are other minimum software requirements that you need to meet for each MOM component. In our scenario here, since we are installing more than one MOM component on one computer, we have to install all the prerequisite software for all the combined MOM components.

Software prerequisites for the MOM 2005 SP1 Management Server are:

- Microsoft Data Access Components (MDAC) version 2.8.1022.0 or later
- Microsoft .NET Framework version 1.1

Prerequisites for the MOM 2005 SP1 Database include:

- Microsoft SQL Server 2000 Standard or Enterprise Edition with Service Pack 3.0a or later

To install the MOM 2005 SP1 Administrator Console and Operator Console, the prerequisites are:

- Microsoft .NET Framework version 1.1
- One of the following browsers: Microsoft Internet Explorer 6 with Service Pack 1, Microsoft Internet Explorer 5.5 with Service Pack 2, or Netscape 4.78 or later

In order to use MOM 2005 SP1 Reporting, the following software prerequisites must be installed:

- Microsoft SQL Server 2000 Standard or Enterprise Edition with Service Pack 3.0a or later
- SQL Server 2000 Reporting Services SP1
- A browser that can render reports in HTML 3.2 and HTML 4.0.
- Microsoft Visual Studio .NET 2003, or Integrated Developer Environment 2003 (if you want to customize or create reports)

In order to use the MOM 2005 SP1 Agent, the following must be installed:

- A supported operating system
- Microsoft .NET Framework version 1.1

Some of the most common prerequisites that the MOM Prerequisite Checker catches in a typical installation scenario such as our example include:

- IIS not installed
- ASP.NET not installed
- SQL Server 2000 SP3 or higher not installed
- SQL Server 2000 Agent Service not set to Automatic
- Background Intelligent Transfer Service not set to Automatic
- COM+ not installed

How to correct each of these problems will be discussed during the installation process section of this chapter.

Shortcuts…

A New Service and a New Book

WSUS, or Microsoft Windows Server Update Services, allows you to deploy Microsoft product updates to Microsoft Windows Server 2000, Windows Server 2003, and Windows XP operating systems easily and efficiently. Using WSUS means you can fully manage the distribution of updates that are released through Microsoft Update to computers in your network. For more information, see *How to Cheat at Managing Windows Server Update Services* (Syngress Publishing, ISBN: 1-59749-027-X).

In addition to making sure that the prerequisites are installed, it's also important that you make sure that all appropriate security updates, hotfixes, and service packs have been applied to the operating system and to the installed applications before you install the desired MOM components. Another suggestion is that if you have a virus checker installed and running on this system, disable it until after you have installed the MOM 2005 components to avoid potential problems.

Best Practices According to Microsoft

- Before installation, use the Performance and Sizing Guide located at http://go.microsoft.com/fwlink/?LinkId=46754 to assist you in determining what size your MOM database should be.
- Install the MOM Database (EeaData.mdf) and log files (EeaLog.ldf) on separate hard drives for greater efficiency. (These should be different hard drives, not just different partitions.)
- Install the SQL Server database and log files for MOM on a different hard drive than the paging file. The paging file usually is located on the same drive as the operating system.

Some Independent Advice

It might be a good idea to take these Best Practices one step further for not only greater efficiency but redundancy of data. Not only should you install the database and log files on different hard drives but you might want to have those hard drives on different hard drive controller cards also. In our example machine then you would have one hard drive and controller card for the operating system and paging file, a second hard drive and controller card for the MOM database, and a third hard drive and controller card for the log files. As you may be beginning to see, placing all the MOM 2005 components on a single machine requires the machine to have considerable resources.

If the computer does not have the required software and hardware you have two choices: either remove it from your deployment plans or upgrade the required hardware and install the required software.

One other step that you should complete before moving on to installing the various components is to verify the MOM 2005 Service accounts. There are three primary service accounts used by MOM 2005:

- The Data Access Server (DAS) account
- The Management Server Action Account
- The Agent Action Account

Shortcuts…

Use Windows Update First

MOM 2005 Prerequisites can be rather picky during installation. Save yourself time by doing a clean install of the operating system and then immediately using Windows or Microsoft Update to make sure that all your operating system components are up to date.

The DAS account provides centralized access to the MOM 2005 database.

The Management Server Action Account runs computer discovery and automatically installs agents. It also enables the Management Server to communicate with unmanaged servers performing such actions as collecting data from and running actions on those computers. Finally, the Management Server Action Account also can collect data from the registry, performance counters, and event logs of the computer on which the Management Server is installed.

MOM 2005 uses the agent Action account to collect data from and to run actions on agent-managed computers.

BEST PRACTICES ACCORDING TO MICROSOFT

From a security standpoint, it's recommended that different accounts be used for the MOM 2005 Management Server Action Account and the DAS account. Using the same account for several different services opens your system up to complete takeover should that account be compromised. Using separate accounts improves your security in your MOM 2005 environment.

Installing Server Components

Again, in this example installation, all the MOM 2005 components will be installed on one server. Referring to the previous discussion concerning the minimum operating system requirements for a MOM 2005 single server installation, the minimum operating system we can install MOM 2005 on is Windows 2000 Server with Service Pack 4 or later.

For example purposes, this chapter will concentrate on Windows 2000 Server with Service Pack 4 with examples from Windows Server 2003, Enterprise Edition with Service Pack 1 where there are minor differences. We will also use and discuss the use of three different versions of SQL Server and two different versions of MOM 2005. The assumption is made that all installation software is available on CD. If your installation software is on any other media you will need to make the necessary modifications to the following instructions to accommodate your use of a different installation media.

At this point you should have the operating system installed and updated to the required service pack. In addition to the correct service pack you should go to Windows Update or the new Microsoft Update and install all the relevant security updates listed there for your operating system.

One of the main differences between the two operating systems may catch you later and you want to deal with it now so that doesn't happen. MOM 2005 requires that IIS be installed on the system. Windows 2000 Server installs IIS by default. Good security practices have drilled into some of us to uncheck the IIS install by habit so that IIS doesn't get installed during the operating system installation. Windows Server 2003, Enterprise Edition does not install IIS by default during its installation. Whatever operating system you choose to install MOM 2005 onto, make sure that you have IIS installed during the installation to save yourself time later.

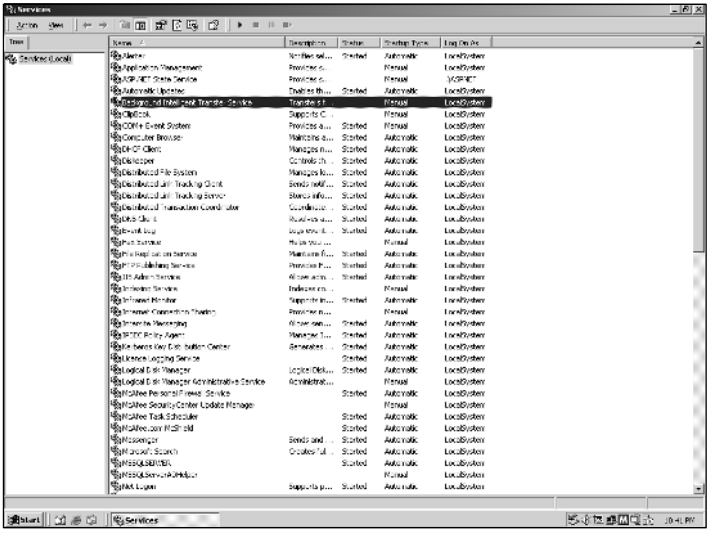
Another common missing component you'll need to deal with, especially on the various versions of Windows 2000 Server, is ASP.NET. The prerequisites for ASP.NET for this installation are IIS, Service Pack 2 or later, Internet Explorer 5.01 or later, and MDAC 2.6 or later. By today's standards, these versions are quite dated but a quick stop at Windows Update or Microsoft Update can more than meet these requirements.

As this is a server installation, the Redistributable version of the Microsoft .NET framework Version 1.1 will be acceptable but Version 2.0 is the current version as of the date of this writing. Download the file from www.microsoft.com/downloads/. The filename is dotnetfx.exe and is just under 24 MB in size.
Installing the Redistributable is a simple, straightforward procedure. Run the executable and you will be asked if you want to install the Microsoft .NET framework or not. You may be asked to agree to the EULA next and then in a short period of time you will receive a message stating that the framework has been installed.

There are a couple of other small "gotcha's" that you need to look for. The first is that MOM 2005 doesn't want to be installed on a domain controller. In fact, the main MOM 2005 component will not run on a domain controller. If the target server is already set up with Active Directory, uninstall it. Otherwise, you will be getting a warning every time you run the MOM Prerequisite Checker.

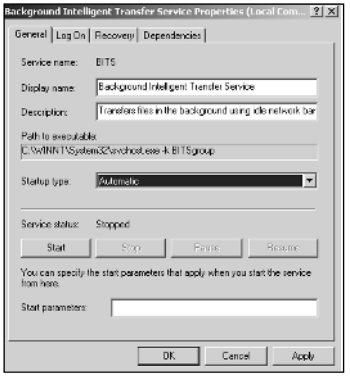
Next, by default, the Background Intelligent Transfer Service is set to manual start, as seen in Figure 4.5. It needs to be set to Automatic.

Figure 4.5 The Background Intelligent Transfer Service in the Services MMC



Changing the setting is easy. Just right-click the service in the MMC and choose Properties from the pop-up menu. On the General Tab, as seen in Figure 4.6, change the Startup type from Manual to Automatic. Click the Apply button and the service will now be set to start automatically in the future. Next, click the **Start Button** and after the service starts click the **OK** button.

Figure 4.6 Change the Startup Type from Manual to Automatic



Another item you might want to go ahead and install at this point in time is Microsoft Data Access Components Version 2.8. Download the latest version from

www.microsoft.com/downloads/ and run the install program. One of the first things you will see is the EULA. Check the box agreeing to the terms and the click the **Next** button. The next window allows you to start the installation process. Next, click **Finish** and after a short period of time you will be asked to restart the computer. Go ahead and click **Finish**. When the system is restarted you should be ready for the next step, installing SQL Server on the machine.

Installing and Preparing SQL Server

SQL Server is an important component of the MOM 2005 installation and the installation must meet specific requirements. You can use either SQL Server Enterprise or Standard. Installing the MOM 2005 database on the Microsoft SQL Server Desktop Engine (MSDE) is not supported. Also, at the time of this writing, SQL Server 2005 is being released to market. Microsoft announced earlier that they would officially support MOM 2005 SP1 on SQL 2005 but this wasn't official at the time of this writing as the MOM development group was still testing for compatibility.

For the purpose of this example installation we will show the steps required to install both versions. We'll start with SQL Server 2000 Enterprise on the Windows 2000 Server with Service Pack 3. There are some minor differences when installing SQL Server 2000 on Windows Server 2003 that will be discussed also. Because this book is not a SQL Server specific book, the discussion here will center specifically on the installation of the SQL Server software and not so much on what the various options that can be chosen would do. We will discuss only those options that are relevant to our MOM 2005 installation process.

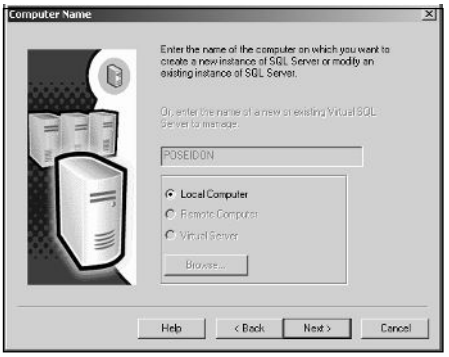
The first step is to place the SQL Server CD into the machine's CD-ROM. The auto-run should automatically start the SQL Server 2000 installation program and the SQL Server Welcome will appear. If you are installing SQL Server 2000 on a Windows Server 2003 system you will also be informed that SQL Server 2000 with less than Service Pack 3 is not compatible with Windows Server 2003. Since MOM 2005 requires SQL Server 2000 with Service Pack 3 don't worry about this message at this point in time. Keep in mind that for production installations, MOM 2005 supports only Microsoft SQL Server 2000 Service Pack 3.0a as the database for the MOM database. You'll be installing Service Pack 3 later in this example scenario.

Click **Next,** and your next choice to make is what computer to install SQL Server on, as shown in Figure 4.7. This option allows you to choose to install SQL Server on:

- The local computer
- A remote computer
- A virtual server

Because this installation is to install all the necessary MOM 2005 components on a single server, choose the local computer option.

Figure 4.7 Choose the Computer on Which You Wish to Install This Instance of SQL Server

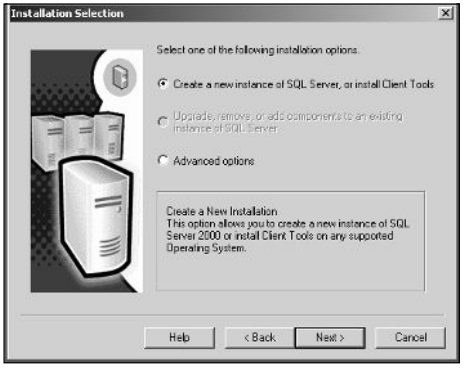


Once you've chosen where to install, the decision must be made as to what this installation will do. As can be seen in Figure 4.8, the options presented are:

- Create a new instance of SQL Server, or install Client Tools
- Upgrade, remove, or add components to an existing instance of SQL Server
- Advanced options

The default is **Create a new instance of SQL Server, or install Client Tools** and this is the option you want to use in this installation.

Figure 4.8 Choose What Kind of Installation You Wish to Perform



The next three steps of the installation process are the EULA acceptance, entering the CD-Key, and entering your name and company. You first are asked to

accept the Software License Agreement. Accept the license agreement by clicking **Yes**. Choosing not to accept the license agreement will end the installation process at this point.

Next, the process allows you to enter the CD-Key. Make sure you enter it correctly and then click the **Next** button. Entering an incorrect CD-Key at this point will halt the installation process until you provide the correct information.

Finally, the next dialog window in this group allows you to enter your user information. Although the company name is not required, it is a good practice to enter it here to help with server identification in the future. Enter your name and your company and click **Next** to proceed.

The next step is to define the process. As can be seen in Figure 4.9, the options here are to install:

- Client Tools Only
- Server and Client Tools
- Connectivity Only

The default option, and the one to be used in this installation, is to install the Server and Client Tools. Click **Next**.

Figure 4.9 Defining the Installation Process

The three different types of setup that can be used are shown in Figure 4.10 and listed here:

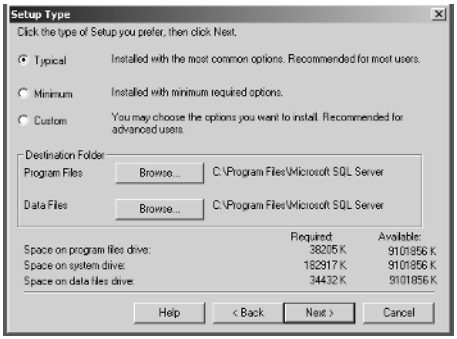
- **Typical** This installation option installs the most common options available and is recommended for most users.
- **Minimum** This installation option installs only the minimum required options.

- **Custom** This installation option allows you to choose what options you wish to install and is recommended only for advanced users.

You are also given the opportunity to assign the locations of both the SQL Server program files and the data files. Unlike in Figure 4.10, best practices suggest installing the two groups on separate hard drives. You would also probably want to make sure that the two hard drives are on different controllers and that they are on different drives than the drive containing your operating system or your paging file.

You should probably accept the default **Typical Setup** but, as discussed earlier, configure your destination folders for redundancy and for reliability. Once these choices are made, click the **Next** button.

Figure 4.10 How and Where Do You Want to Install the SQL Server Software?



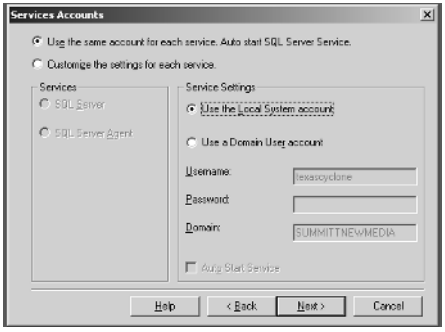
The next step is to choose the accounts that will be used to administer the SQL Server services. As can be seen in Figure 4.11, the first choice you have to make is to use the same account for each service and auto-start the SQL Server service or to Customize the settings for each service. The level of security you want for the SQL Server services will determine the choice you make at this point. In our example scenario here we have chosen to use the same account for each service. This simplifies the administration process.

The next step on this dialog window requires you to choose the local system account or a domain user account to be associated with the service or services. The default is to choose a domain user account. In our installation scenario we have chosen to use the local system account to simplify administration in this example scenario. There are reasons why you might want to run the SQL Server service under a domain user account though. Many server-to-server activities can only be performed with a domain user account. These activities might include remote procedure calls, replication, backups, or even heterogeneous joins that involve remote data

sources. If you are not sure just which type of user account you want to use, read the sections dealing with user accounts in the SQL Server Books Online.

After you have made your selections click **Next** to move to the next step of the installation process.

Figure 4.11 Choose Your Service Accounts

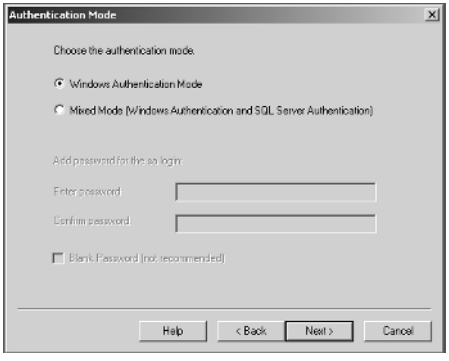


The next step of the installation process involves choosing the Authentication mode you wish to use. As with some of the previous steps in this process, your choice is determined by the level of security you wish used with your installation. The two options are:

- Windows Authentication Mode
- Mixed Mode (Windows Authentication and SQL Server Authentication)

To work properly with MOM 2005, the authentication mode must be set to Windows Authentication Mode only. Choose the option you wish to use with your installation in Figure 4.12 and click **Next**.

Figure 4.12 Choosing the Authentication Mode

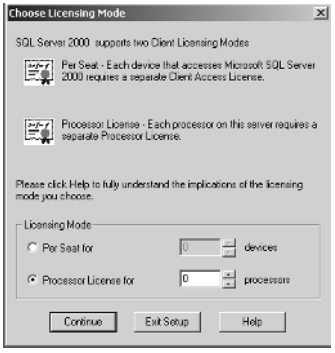


The installation process now has enough information to move on to the next step, that of you providing licensing information to the process. Click **Back** if you want to review or change the settings you have provided up to this point. Otherwise, click **Next** to move to the Licensing dialog window.

The Licensing mode dialog window, as seen in Figure 4.13, allows you to choose Per Seat or Processor License. The Per Seat option requires that each computer that connects to the SQL Server requires a separate Client Access License. The Processor License option requires that each processor on the server hosting the SQL Server installation have a separate processor license.

Check the type of license that was purchased with your specific SQL Server software and choose the option your installation requires. Click **Continue** after you have made your choice and specified either the number of devices or the number of processors.

Figure 4.13 Choose Your Licensing Mode



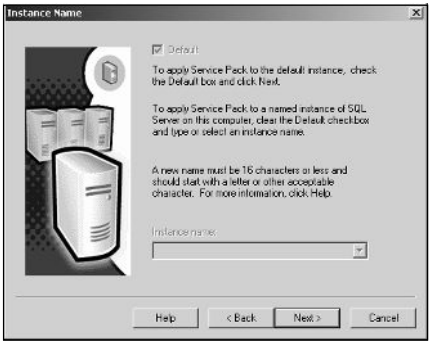
The installation process has now started. Click **Finish** on the Setup Complete dialog window to complete the SQL Server installation.

Your installation of SQL Server 2000 is complete, but as was discussed earlier, MOM 2005 (and Windows 2003 Server if that is the operating system you are using) requires at least Service Pack 3 for SQL Server 2000 to be installed. Take your SQL Server 2000 CD out of the target system CD-ROM and put in your Service Pack CD. At the time of this writing, Service Pack 4 for SQL Server 2000 is also available, but as discussed earlier, Service Pack 3.0a is the only Service Pack supported for the MOM 2005 database. As a result, for this example scenario Service Pack 3.0a will be used.

Start the Service Pack installation and you will be greeted with a screen similar to the Welcome screen you saw previously installing SQL Server 2000. The difference is that this screen identifies the Service Pack number.

Many of the dialog windows you will see in the Service Pack installation will be similar in the same respect as those you saw in the installation of SQL Server. There are a few exceptions though. The EULA dialog window is the same but your next step is to choose the instance to which the Service Pack will be applied as seen in Figure 4.14. It is possible to have multiple instances on a server with different Service Packs applied, so be aware of what instances you have installed on a given server.

Figure 4.14 Choose the Instance to Which the Service Pack Will Be Applied



In our example scenario, as probably in your situation, the default instance is the only instance on the machine and therefore is selected by default. Click the **Next** button.

The next dialog window asks how the Service Pack installation should connect to the SQL Server instance. Your choice in the Connect to Server Dialog Window, as seen in Figure 4.15, will be determined by what your choices were on the Service Accounts and Authentication Dialog Windows in the SQL Server installation previously as seen in Figures 4.11 and 4.12. As described earlier, for this example scenario the Windows account information was chosen with Windows Authentication. Click **Next** when you have made your selection.

Figure 4.15 Your Choice Here Will Be Determined by Your Previous Decisions

A common security problem with SQL Server 2000 is that the SA account usually is installed with no password. Service Pack 3 and later correct this problem. The next dialog window that will appear in the process is the SA Password Warning dialog window such as that seen in Figure 4.16.

Figure 4.16 Set the SA Password to Increase Security

Enter a password in both textboxes and click **OK**.

Best Practices According to Microsoft

- You might want to check into the Microsoft SQL Server Best Practices Analyzer. This free download is a database management tool that lets you verify the implementation of common Best Practices for SQL Server according to Microsoft. Generally, these best practices deal with the usage and administrative aspects of SQL Server databases. They also help to ensure that your SQL Servers are managed and operated well.
- You can download this free tool at www.microsoft.com/downloads/details.aspx?FamilyId=B352EB1F-D3CA-44EE-893E-9E07339C1F22&displaylang=en.

The next dialog window deals with setting up the Service Pack. There are two choices you need to make. As seen in Figure 4.17, you have the opportunity to enable cross-database ownership chaining for all databases and to upgrade Microsoft Search and apply the service pack to it. The first option is not recommended and the second option is required. Click **Continue** to move to the next dialog window.

The next dialog window deals with SQL Server error reporting. Should the SQL Server encounter a fatal error during operation, the server can send information about the error directly to Microsoft over a secure connection. To enable the sending of these reports check the box in the lower right corner of the dialog window, as seen in Figure 4.18, and then click **OK**. If you wish to control the information sent to Microsoft, visit http://oca.microsoft.com/cerintro.asp.

Figure 4.17 Make Sure the First Option Is Unchecked and the Second Is Checked

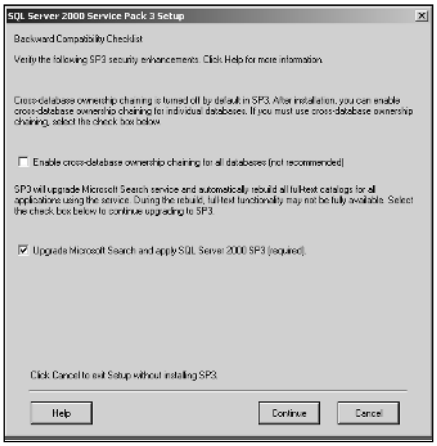
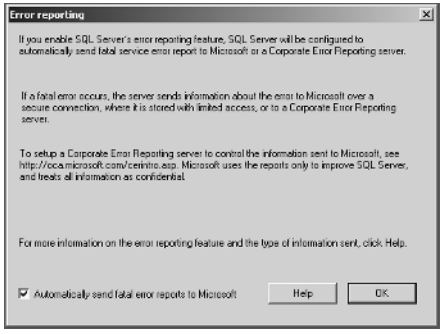


Figure 4.18 Do You Want to Notify Microsoft of Any Fatal Errors Your SQL Server May Encounter?



You are now finished entering the information needed by the setup program to install the Service Pack and will be informed of this by the Start Copying Files dialog window. Click the **Next** button and the Service Pack will be installed. In a relatively short period of time, depending on the speed of your hardware, you will have completed the installation of the SQL Server and the Service Pack. Verify that the default SQL Server databases have been installed before you go any further. This is accomplished easily by opening the SQL Server Enterprise Manager and connecting to the SQL Server instance that will be used. Make sure that the Tempdb, master, and msdb databases are installed.

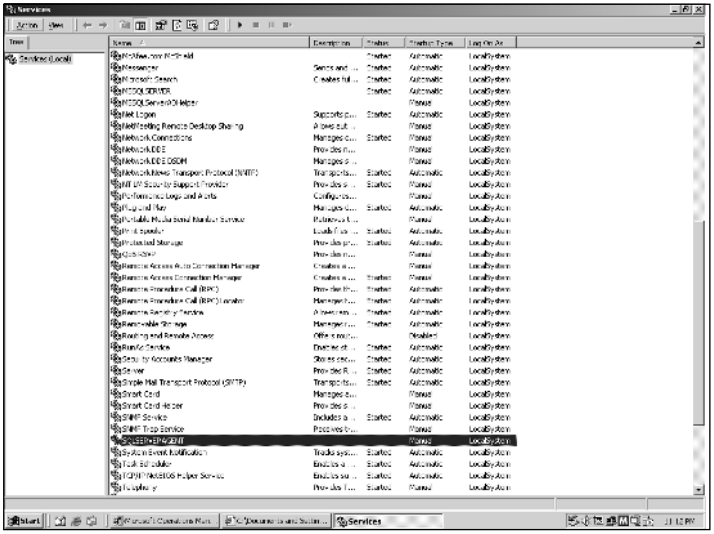
Best Practices According to Microsoft

Sufficient memory should be installed to meet the system's needs, but in situations where the memory is limited Microsoft recommends that you configure the database to handle such processes that might use all the memory as well as those that might cause page faults. SQL Server uses as much unallocated RAM as it requires. It will then release RAM as needed for other resources. The only way to prevent this is to limit the amount of memory that SQL Server uses by configuring the memory as static rather than dynamic. Keep in mind that doing this will result in reduced MOM 2005 performance.

You've now completed the installation of the operating system and all updates and service packs required for the successful installation of MOM 2005. But there may still be one gotcha that you'll need to deal with.

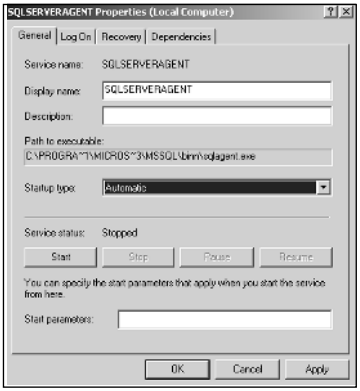
SQL Server installs with the MSSQLSERVER service startup type set to Automatic by default. The SQLSERVERAGENT service startup type, however, is set to Manual by default. MOM 2005 requires both to be set to Automatic. This is a rather simple procedure and is accomplished by starting up the Services MMC, as seen in Figure 4.19.

Figure 4.19 Select the SQLSERVERAGENT Service in the MMC



Right-click the **SQLSERVERAGENT** and choose **Properties.** You will see the Properties dialog window, as in Figure 4.20.

Figure 4.20 Change the Startup Type from Manual to Automatic

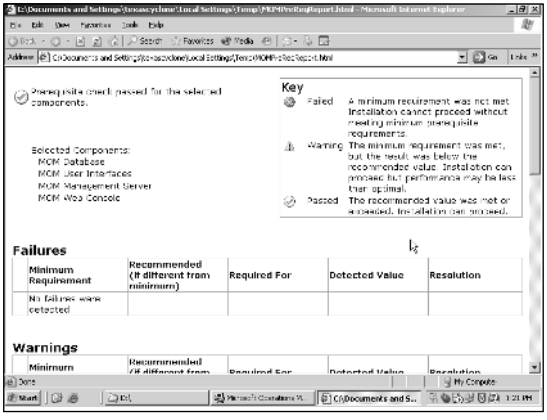


Change the Startup Type from Manual to Automatic and then click the **Apply** button. Now click the **Start** button if the service is stopped. It will take just a moment for the service to start and then you can click **OK** exiting the Properties dialog window. Close the Services MMC. It's now time to start the MOM 2005 installation process.

Installing MOM Components

Place your MOM 2005 installation CD in the target machine's CD-ROM. You should probably run the MOM Prerequisite Checker one more time just to verify that everything is installed as required and that, as in Figure 4.21, your installation target has no Failures or Warnings.

Figure 4.21 No Failures, No Warnings



If there are still any failures or warnings go back and correct them now because although MOM 2005 may install with warnings, there may be problems with the

installation in the future. So the best bet is, as was suggested, to go ahead and correct these failures and warnings now.

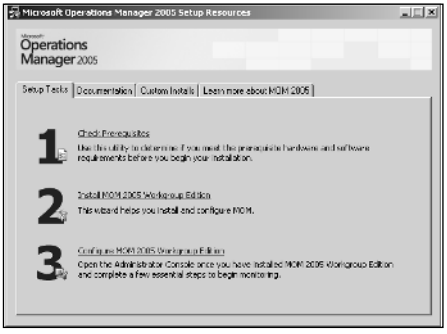
The next step is to start the MOM 2005 installation. Click the second option on the MOM 2005 Setup Resources dialog window, as seen in Figure 4.22.

Shortcuts…

A Word about the Screenshots

The graphics used in this discussion of the installation of MOM 2005 are from both the MOM 2005 Workgroup version and the MOM 2005 Standard version. Most of the dialog windows are similar in all versions of the software, and we will show both when the different versions diverge.

Figure 4.22 Install MOM 2005 Now by Choosing the Second Option Available on Your MOM 2005 Setup Resources Dialog Window



The next window you will see is the MOM 2005 setup wizard. Click **Next** and move on to the next step of the installation process.

The next step in the installation process is that of agreeing to Microsoft's End-User License Agreement. Check the radio button in front of the statement "I accept the terms of the license agreement." Click the **Next** button after agreeing and move on to the next step of the process.

Depending on what version of the MOM 2005 software you are installing, the license terms may be a little different and will state what version of the software you are installing. In any event, choose the "I accept the terms in the license agreement" radio button and click **Next**. If you choose not to accept the license, the setup program will close. The next step, if you are installing any version other than the

evaluation version, requires you to enter the 25-digit CD-Key. In most cases you should find the key on the back of the CD case, but you may have a yellow sticker with the code.

After entering your code, click the **Next** button. The next dialog window will depend on what version of the software you are installing. If you are installing the Workgroup edition, as seen in Figure 4.39, you will now be allowed to choose where you want the MOM 2005 files installed. This decision should have been made during the planning phase. Developing a good plan for the installation is extremely important and following that plan is even more important.

You can change where you are going to install MOM 2005 by clicking **Browse** and choosing a different location than that listed on the dialog window. You might want to check how much free space you have on your hard drives before you place the files on any specific drive. During one of our installs the plan called for installing the files on the C drive as listed in Figure 4.23. By clicking the **Disk Usage** button and examining the results as shown in Figure 4.24, we determined that placing the MOM 2005 files on the C drive would not be the best use of the system.

Figure 4.23 Where Are You Going to Install MOM 2005?

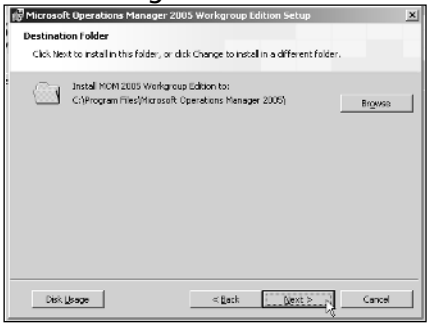
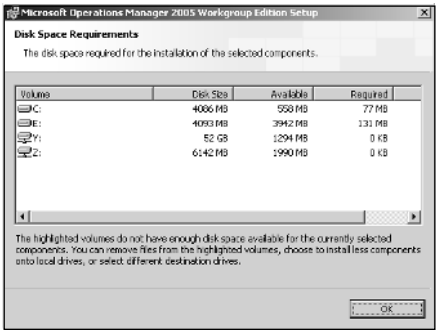


Figure 4.24 Examine the Disk Space Requirements



Once you have determined if the drive has enough space available to install MOM 2005 or not (if you try to install on a drive that does not have enough space, the installer will notify you of the situation), click **OK** and return to Figure 4.23. Make the necessary changes to your installation there and then click **Next**.

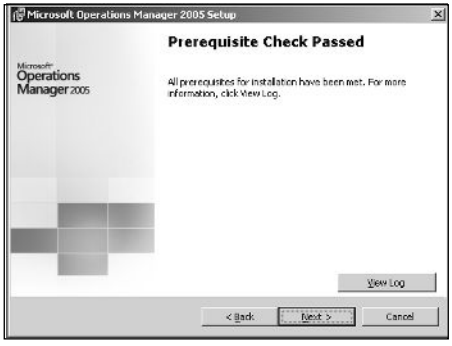
If you are installing MOM 2005 Standard edition, you will be given the opportunity to choose typical or Custom installation, as in Figure 4.25.

Figure 4.25 Choose Typical or Custom Installation

Choosing the Custom installation will give you similar options to those discussed previously regarding the Workgroup Edition. This type of installation is used primarily for installing the various MOM 2005 components on different computers. We will be discussing this choice more fully in the next section of this chapter when we discuss installing the MOM 2005 components on different machines. For this scenario, go ahead and choose the Typical installation and click the **Next** button.

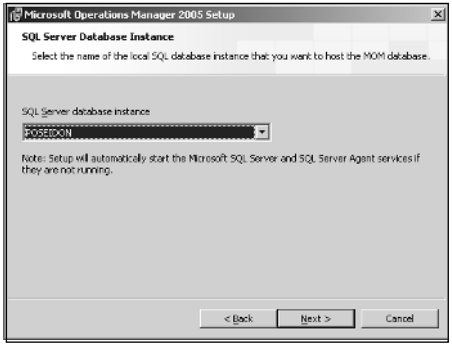
The MOM 2005 Standard Version will now check the prerequisites for you again, as seen in Figure 4.26.

Figure 4.26 The Installation Will Check the Prerequisites for You Again



If there have been any failures click the **View Log** button, find out what they are, correct the problems, and restart the MOM 2005 installation. If all the prerequisites for installation have been met, as in Figure 4.26, click the **Next** button. Both versions, the Workgroup Version and the Standard Version, will now converge again and you will be offered the opportunity to select what database instance you want to use, as shown in Figure 4.27.

Figure 4.27 Choosing Your Database Instance

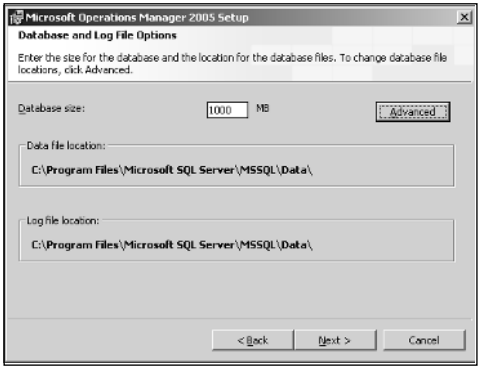


There shouldn't be but one instance since this is a new install of SQL Server but you might want to check the drop-down list just in case. Choose the instance and click **Next**.

The two versions, the Workgroup and Standard, will diverge again for a moment. If you are installing the Standard version the next dialog Window you see will look similar to Figure 4.28.

This dialog window allows you to determine how big your MOM 2005 database will be and where the data files and log files will be located. The default setting for the database size is 1 GB (1000 MB).

Figure 4.28 Change the Database Size and File Locations



You can, and should, change the amount and then their locations by clicking the **Advanced** button and then clicking the **Change** button as seen in Figure 4.29.

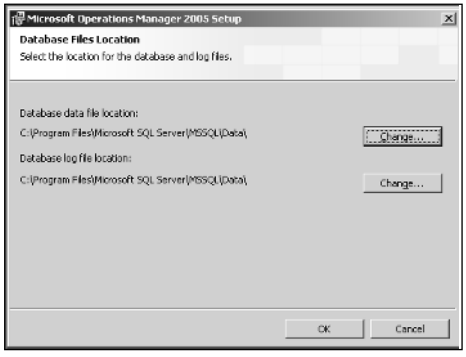
Some Independent Advice

The MOM 2005 installation process installs the data file and log file on the same hard disk drive by default. You should change this setting to install them on different drives. Another suggestion is that neither file be installed on the same disk as the operating system's paging file.

The minimum and maximum supported size for the MOM 2005 database is 300 MB and 30 GB, respectively. A smaller size database will provide better performance so you should probably consider maintaining the database size between 12 and 15 GB.

One other point to remember is that the size of the log file is set to 20 percent of the size of the data file automatically by the MOM 2005 installation process. So if the data file is set to 10 GB then the log file size will automatically be set to 2 GB.

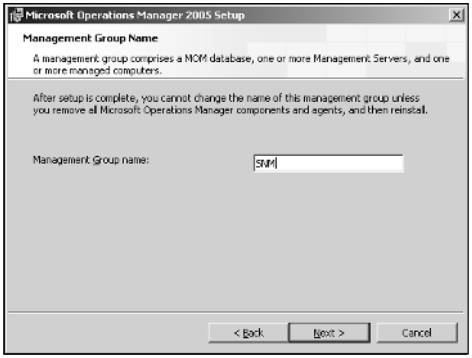
Figure 4.29 Change the Data and Log File Locations



Click **OK** after you have changed the file locations and you will return to Figure 4.28. After you have decided what size the database will be and where the files will be located click the **Next** button.

Figure 4.30 shows the next dialog window you will see in the Standard version. This dialog window allows you to enter a Management Group name. After the installation is complete you won't be able to change the name of this group without completely uninstalling all MOM components and agents and then reinstalling the application so choose this name carefully. Click **Next**.

Figure 4.30 Choose Your Management Group Name



The two versions of MOM 2005 will now converge again, and Figure 4.31 displays the next dialog window you will see. This dialog window requires that you provide a User Account and its password via which you will be administering the MOM 2005 Server. Do not provide an administrator account here. When you have provided the required information, click **Next**.

Figure 4.31 What User Account Will You Use to Manage MOM 2005?

The Standard version will diverge again as in Figure 4.32.

You will need to notify the installation here if you have Active Directory installed or not. The MOM 2005 Standard installation recommends that the Active Directory option be selected but you can choose not to use Active Directory if you wish. Click the **Next** button after you have made your choice.

The two versions converge again and you will now see a dialog window similar to Figure 4.33.

Figure 4.32 Active Directory or Not?

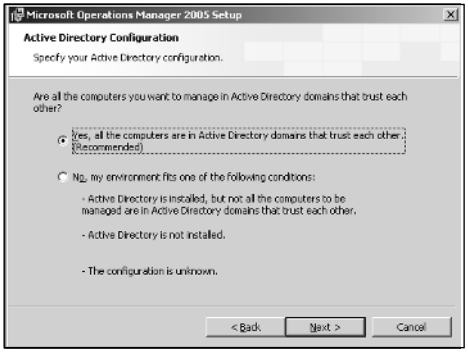
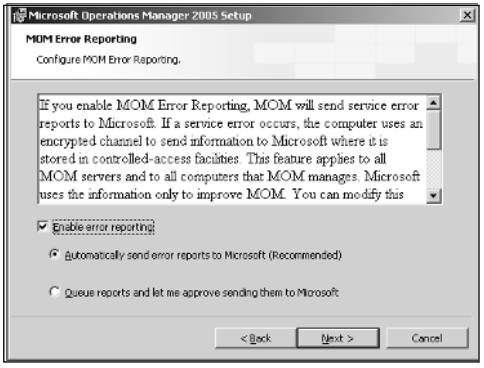


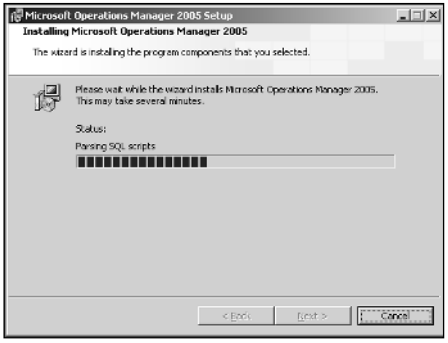
Figure 4.33 Configure MOM 2005 Error Reporting



As Figure 4.33 indicates, you are now able to decide if you want to enable error reporting from MOM 2005 or not. Enabling error reporting sends an encrypted message to Microsoft containing information concerning the error. Your decision here is based primarily on how you feel about the big mean ogre called Microsoft. If you hate them, why use the product? If you are interested in helping them to improve the product, check the box and send the reports. If you don't know, queue the reports and decide if you want to send the reports or not later. For now, make some sort of a decision as to whether you want to send these messages or not and click **Next**. You're now ready to begin the installation of MOM 2005. Click the **Install** button.

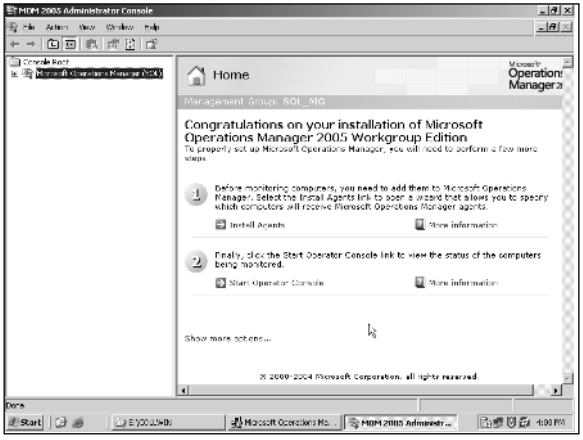
The installation will take some time, as seen in Figure 4.34, depending on the software options you have chosen and the hardware you are installing to. When the installation completes, make sure that the Start the MOM Administrator console checkbox is checked and then click **Finish**.

Figure 4.34 The Installation May Take Some Time



The MOM 2005 Administrator Console, as shown in Figure 4.35, should appear at this point in time. You want to make sure that your installation has completed correctly to this point before going any further. The reasons for this are that, as with the earlier admonition to make sure that all the updates and service packs were installed before you began the installation, it will save you time in the long run to verify that everything you have done to this point has completed successfully before moving forward.

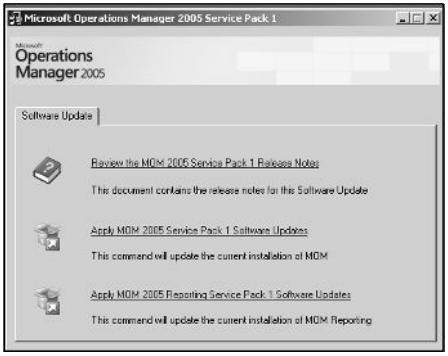
Figure 4.35 Verify that the MOM 2005 Administrator Console Is Available at This Point



The next step in the installation process is to install the MOM 2005 Service Pack 1. You also could perform this step after installing reporting services and discovering the agents, but performing it now will mean you don't have to apply the service pack to any agents you have installed later. Place the CD containing the Service Pack in your CD-ROM and it should start the installation automatically. If it

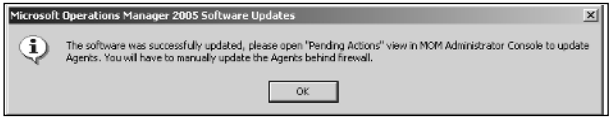
doesn't, or you are not using a CD-ROM, navigate to the location where the Service Pack installation files are located and click **Setup**. The first dialog window you will see will look somewhat like Figure 4.36.

Figure 4.36 Choose the Apply MOM 2005 Service Pack 1 Software Updates



Click **Apply MOM 2005 Service Pack 1 Software Updates** to start the update process. The Welcome splash screen will now appear. Click **Next** and move on. You'll need to agree to the supplemental end user license agreement by clicking the radio button in front of I accept the terms of the license agreement and then you will be able to click **Update**. After a short wait the service pack will be installed. Clicking **Finish** will bring up the dialog window shown in Figure 4.37.

Figure 4.37 You Still May Have Some Pending Actions That Need to Be Performed



If you have already installed reporting services and discovered computers you may need to apply the service pack to the agents. You can open the Pending Actions view in the MOM 2005 Administrator Console to update those agents. At this point in time, you can apply the Service Pack before discovering computers. Later service packs will have to be applied afterward and you may also have to manually update any agents that are behind firewalls.

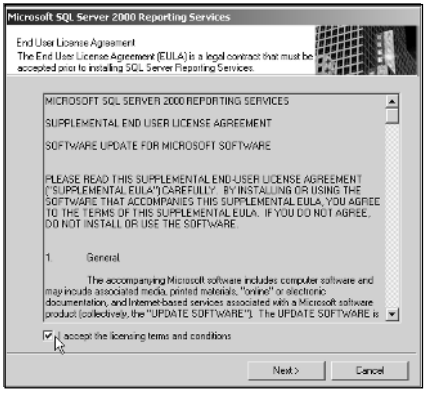
Installing Reporting

It's time now to install Reporting on this machine. In order to install MOM 2005 Reporting Services, you must first install Microsoft SQL Server 2000 Reporting

Services. In the next few pages we will first discuss the installation of the SQL Server 2000 Reporting Services and then that of the MOM 2005 Reporting Services. We will also update the MOM 2005 Reporting Services to MOM 2005 Service Pack 1.

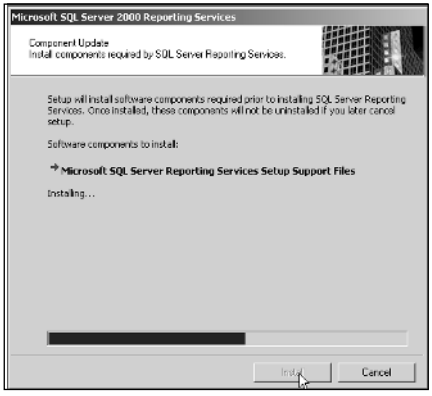
Either put the CD containing Microsoft SQL Server 2000 Reporting Services in your CD-ROM and allow it to auto-start, or navigate to the location of the installation files and click the setup file. The licensing terms and conditions agreement, as seen in Figure 4.38, will appear on the screen.

Figure 4.38 You Must First Accept the Licensing Terms and Conditions



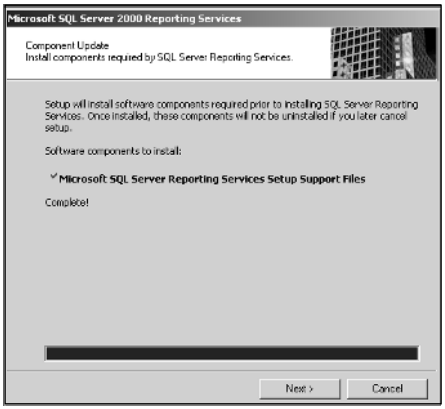
Check the box and click **Next**. The installation and setup support files will now be installed and copied to your hard drive as seen in Figure 4.39. This procedure can take several minutes.

Figure 4.39 Installing the Setup Support Files



When the files all have been copied the application will notify you, as seen in Figure 4.40.

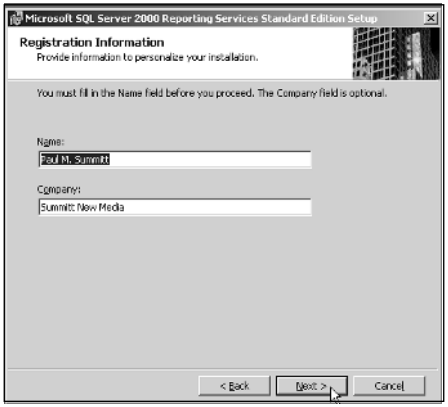
Figure 4.40 The Installation Process in Action



At this point, you have copied only the setup support files to the plane. Click **Next** to start the Reporting Services installation process. Click **Next** to continue installing SQL Reporting Services.

The Registration Information dialog window requires that you enter a name but the company is optional (see Figure 4.41). Usually, depending on the standard procedures under which your company operates, the name should be of that person responsible for the instance of SQL Server. The company could be either the corporate name or the department to which this system is assigned. Click **Next** after you have entered the necessary information.

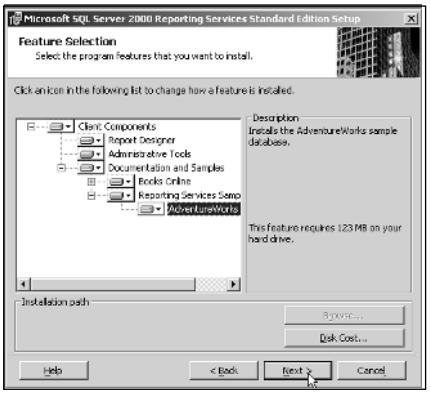
Figure 4.41 Enter the Name of the Person Responsible for the Installation



The Feature Selection dialog window, as seen in Figure 4.42, allows you to choose what components of SQL Server 2000 Reporting Services you want installed. The sample database is an excellent place to learn how to use Reporting

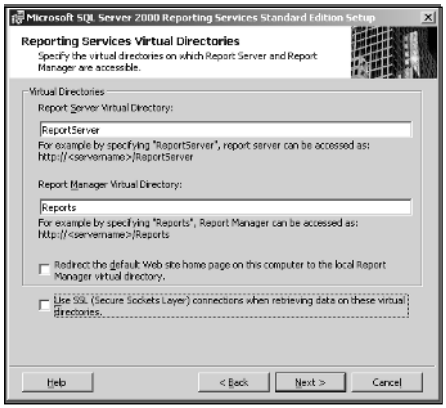
Services if you have not used it before. After you have made your selection, click **Next**.

Figure 4.42 Choose What Components You Want Installed



The next step in the installation process is to choose the virtual directories for the Report Server and the Report Manager. In Figure 4.43, we have accepted the default values. You can also redirect the default Web site home page for this server to the local Report Manager virtual directory by checking the checkbox near the bottom of the Virtual Directories group.

Figure 4.43 Selecting the Virtual Directories

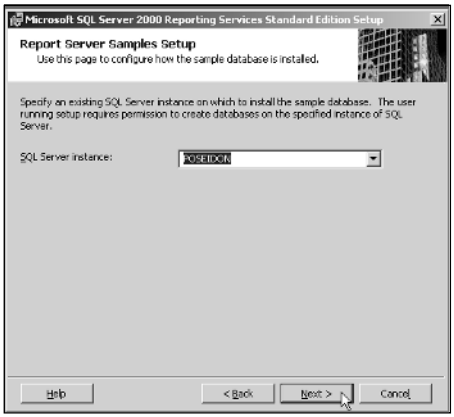


Another option you can choose on this dialog window is whether you will use Secure Sockets Layer connections or not. This checkbox is selected by default. It is recommended for production servers that this checkbox remained checked. For this sample installation we have unchecked it for example purposes only.

After making your choices, click **Next**.

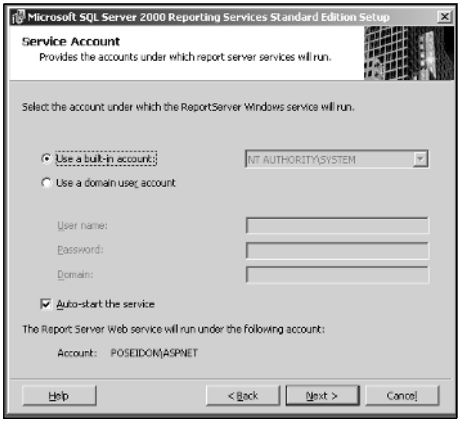
If you choose to install the sample database you will now be offered the opportunity to choose where to install the samples, as seen in Figure 4.44. As in our sample scenario, this is a clean install; there will be only one instance in which to install the samples. Click **Next**.

Figure 4.44 Choose Which Instance for the Sample Database to Be Installed



If you have already installed SQL Server 2000 Service Pack 3 or later, you'll be required to choose which account the ReportServer service will run under, as shown in Figure 4.45. Choose if you want to use a built-in account or a domain user account. If you choose the domain user account, you'll need to enter the user name, password, and domain for that user.

Figure 4.45 You May Be Required to Provide a Password



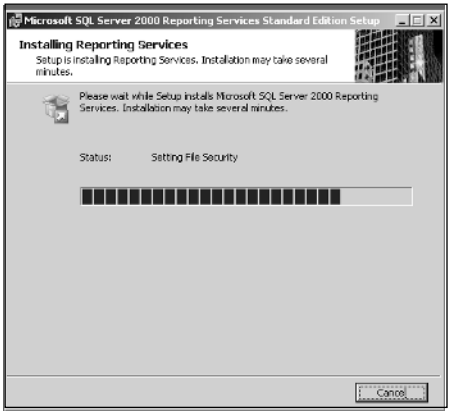
Some Independent Advice

The type of account you decide to use is to a large degree a personal choice, but it also will depend on the needs of the software and your security needs. You know better than any consultant or book what the security needs of your environment are. The default choice is to use a built-in account. In most cases that would not be my choice for a production server. For your test server in this scenario, go ahead and use the built-in account. Before you put your production system into play, examine this option carefully before making a decision.

You can also choose to auto-start the service from this dialog window. If you haven't installed the SQL Server service pack 3 or later yet, you won't see this dialog window.

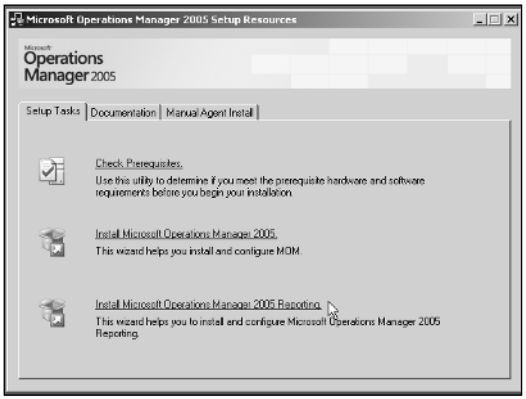
At this point, you're now ready to begin the actual installation. Click the **Install** button to proceed. The installation process will take several minutes but, as can be seen in Figure 4.46, you will be kept informed of the status of the installation. SQL Server 2000 Reporting Services is now installed on your server. The next step of the process is to install MOM 2005 Reporting Services. The process starts when you put the MOM 2005 installation CD back into the server's CD-ROM.

Figure 4.46 The Installation Will Keep You Informed of Its Progress



As with other aspects of the MOM 2005 installation, the Welcome screen will appear on your display as seen in Figure 4.47, and you should select the MOM 2005 Reporting option at the bottom of the dialog window.

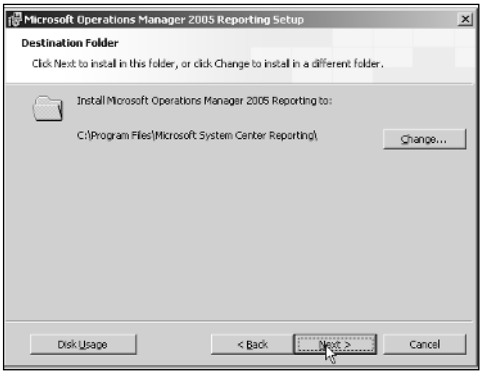
Figure 4.47 Installing MOM 2005 Reporting Services



Click the Install Microsoft Operations Manager 2005 Reporting option to start the installation process. The Welcome dialog window will appear. Close all other programs and click **Next**. At this point you are asked to enter your name, and optionally, your company name. When finished, click **Next** again.

This will bring up the Destination Folder dialog window, as seen in Figure 4.48. By default the installation will place the files in your system drive Program Files folder, but you can click the **Change** button if you want to change this location. Either accept the default or change the location and click **Next**.

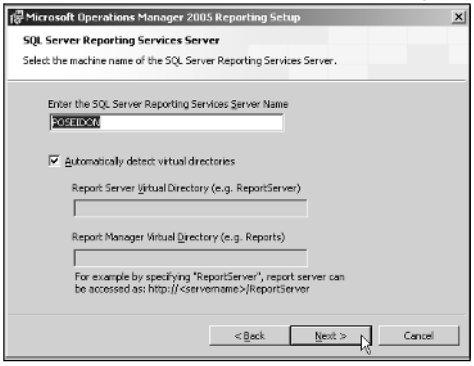
Figure 4.48 Choose Where You Want the Reporting Files to Be Installed



The SQL Server Reporting Services Server dialog window, as seen in Figure 4.49, allows you to choose which SQL Server to use and to automatically detect the virtual directories for the Report Server and the Report Manager. Choose the server and click **Next**. At this point, you should have met all the prerequisites for MOM 2005 Reporting services. If the check has failed, click the **View Log** button

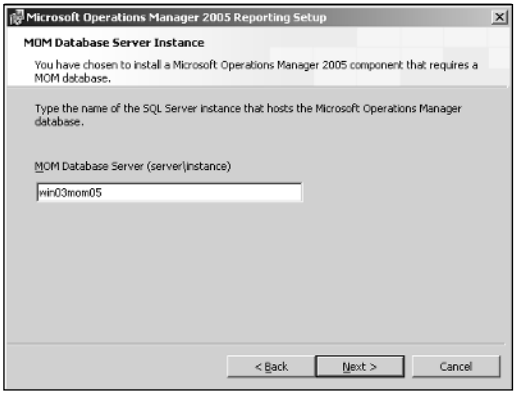
and examine the information to discover what needs to be done for the system to pass the check. If your system has passed the check, click **Next**.

Figure 4.49 Select the SQL Server to Be Used for Reporting Services



Reporting Services requires that you tell it where the MOM 2005 database is, as in Figure 4.50. Enter the name of the database server where the MOM 2005 database is installed and click **Next**.

Figure 4.50 Choose the SQL Server Instance That Hosts the MOM 2005 Database



The next step is to identify for the installation process which SQL Server database instance is to be used, as seen in Figure 4.51. Choose the instance and click **Next**.

The next step, as seen in Figure 4.52, requires that you provide a domain user account that has access to both the MOM 2005 database and to the MOM 2005 Reporting database. Enter the username, the password, and the domain or local computer name and click **Next**.

Figure 4.51 Choose the SQL Server Database Instance

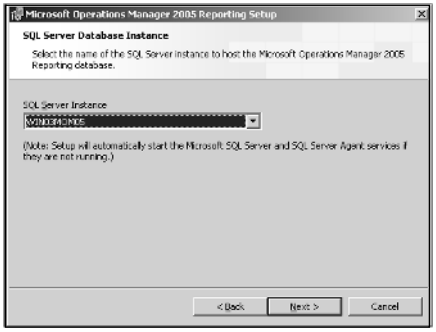
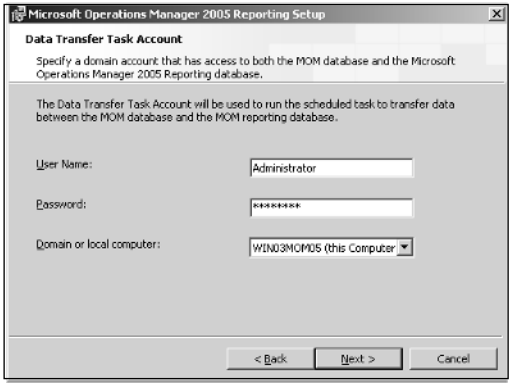
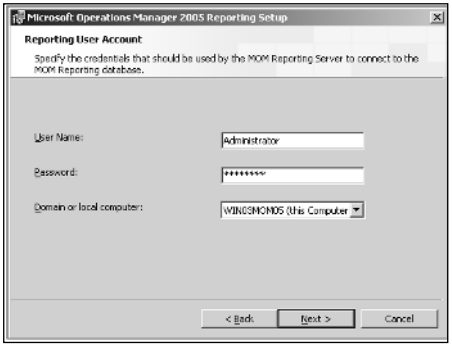


Figure 4.52 Specify a Domain User Account with Access to both the MOM 2005 Database and the MOM 2005 Reporting Database



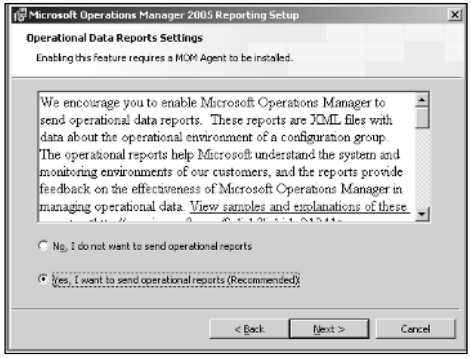
Now, as seen in Figure 4.53, you need to specify a username, password, and domain for an account that will be used by the MOM Reporting Server to connect to the MOM Reporting database. After entering the information, click **Next**.

Figure 4.53 Specify the User to Be Used to Connect to the MOM Reporting Database



The next dialog window, as seen in Figure 4.54, recommends that you submit operational reports to Microsoft. Choose one of the options and then click **Next**. At this point you are now ready to complete the installation. Click the **Install** button. The process will now complete the installation.

Figure 4.54 Do You Want to Send Reports to Microsoft or Not?



Discovering Computers

One of the first things you will want to do with all the target computers you expect to manage is to increase the size of the log files on those computers. If event logging stops on the target computer, MOM 2005 can't pick up the latest events until the logs have been manually cleared and new events are being logged. During this time frame, important information concerning the health of the managed computer may not be reported. If the security log fills up, the managed computer might lock up.

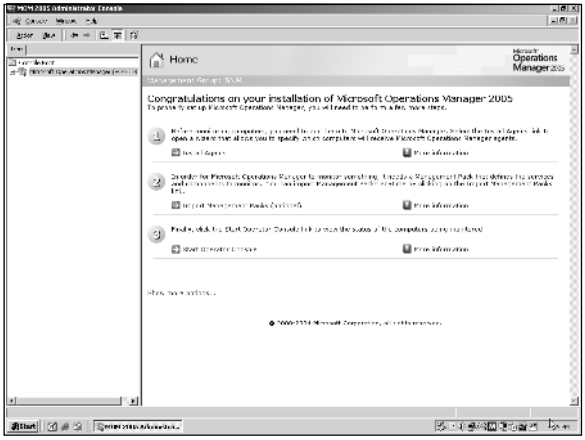
You should therefore increase the size of

- All Windows Event logs
- Event logs for such services as Directory Services, File Replication, and DNS
- Any other application logs such as Microsoft Internet Information Services (IIS) log files

Set the Application, System, and Security logs to at least 25 MB and configure the logs to overwrite events as needed. Keep in mind that this may result in some of the security events being overwritten and therefore lost. Make sure that you know and follow your company's policies regarding security event logging.

The easiest way to discover computers is to open the MOM 2005 Administrator Console, as seen in Figure 4.55.

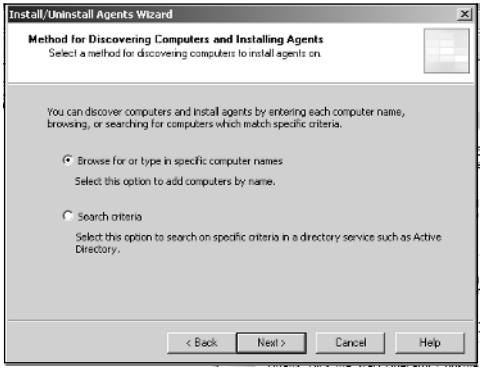
Figure 4.55 Open the MOM 2005 Administrator Console



Click the **Install Agents** option. This will start the Install/Uninstall Agents Wizard. Click **Next** to start the process.

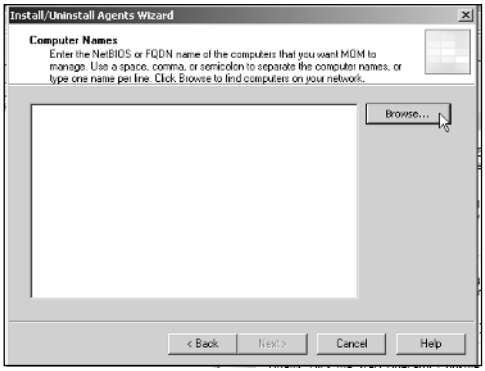
The next dialog window, as seen in Figure 4.56, offers you the option of browsing for specific computer names or to use a directory service such as Active Directory. After you've made your choice, click **Next**. In our scenario here, we have selected to browse for specific computer names, and the next several screen shots will display this option.

Figure 4.56 Choose the Method You Want to Use to Discover the Computers and Install Agents



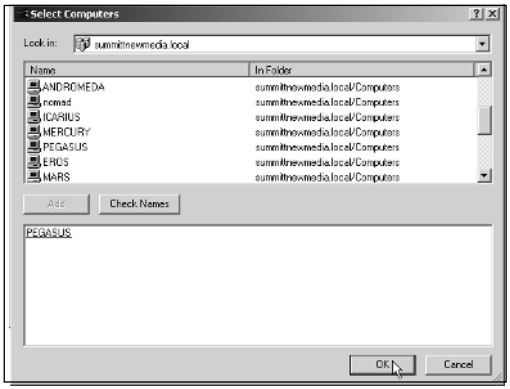
Click **Browse**, as seen in Figure 4.57.

Figure 4.57 Click Browse to Find Computers on Your Network



Select the computer or computers that you want to manage and click **Add**. As seen in Figure 4.58, the computer Pegasus was selected in the top pane and the **Add** button was pressed, moving Pegasus to the bottom pane. After the computer has been added, click **Add**.

Figure 4.58 Select the Computers You Want Managed and Click the Add Button



The fully qualified domain name (FQDN) of the computer we want managed is now displayed in Figure 4.59. Click **Next** to move on.

You now have the choice of what account you will use to install the agents. As seen in Figure 4.60, you can choose either Management Server Action account or Other. If you choose Other you will need to provide the username, in the format domain\username, and the user's password.

Figure 4.59 A Computer Added to the Wizard

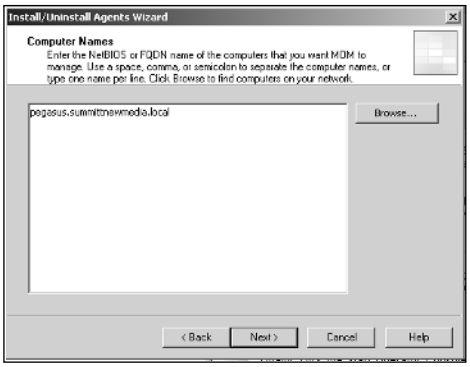
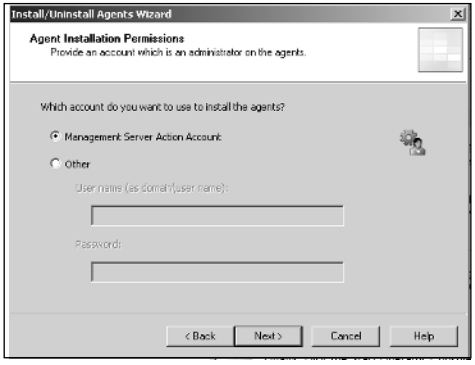


Figure 4.60 What Account Will You Use?

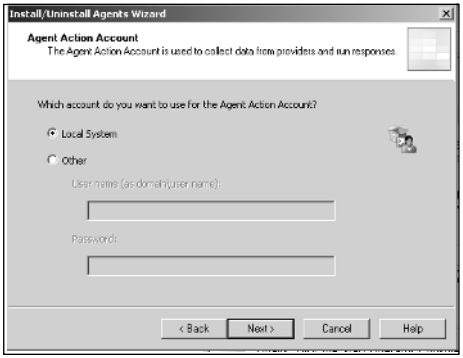


Some Independent Advice

As discussed before in this chapter, your choice of which account to use should depend on the needs of your specific environment and not comments made by a consultant or in a book. You know your systems better than anyone else. In this case, the default is to use the Management Server Action Account. Before changing this to another account, check your environment carefully to make sure that there is no feature that you are using that requires this account to be used. The best advice is to change it from the default only if there is an overriding reason to do so.

Click **Next** to move on to the next dialog window, which provides you the opportunity to choose what account you want to use for the Agent Action Account. As seen in Figure 4.61, your choices are Local System and Other. If you choose Other you will need to provide a username, in the format of domain\username, and that user's password.

Figure 4.61 Which Account Will You Use for the Agent Action Account?

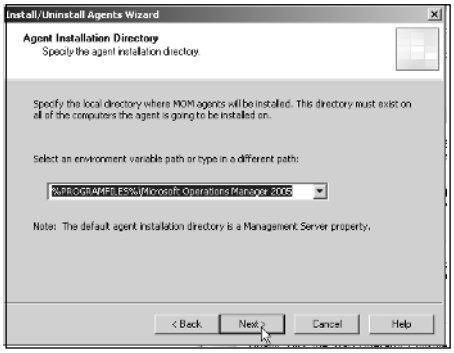


Some Independent Advice

Again, as just discussed, you know your systems better than anyone else. In this case, the default is to use the Local System Account. As stated previously, before changing this to another account, check your environment carefully to make sure that there is no feature that you are using that requires this account to be used. The best advice is to change it from the default only if there is an overriding reason to do so.

After you have made your choice, click **Next** to move on to the next dialog window. This window, as shown in Figure 4.62, allows you to choose where you want the MOM 2005 agents installed. This directory must exist on all computers that are being managed and on the computer where the agent will be installed. As stated in the dialog window, the default agent installation directory is a Management Server property. After you have made any necessary changes, click **Next**.

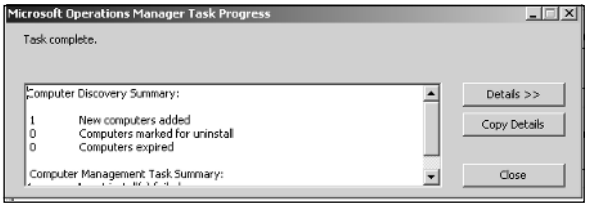
Figure 4.62 Choose the Directory in Which You Want the MOM 2005 Agents Installed



At this point the wizard has gathered all the information it needs to perform the required installations. Show task progress is checked by default. Review your selections in the text window and then click **Finish** to install the agents.

Figure 4.63 shows the dialog window that will be displayed after the new computer has been added to the Management Server.

Figure 4.63 The Installation of the Agent Is Finished



Installing on Multiple MOM Servers

As discussed earlier in the chapter, the first step in preparing to install Microsoft Operations Manager is to verify that the computers selected to host the various components of the MOM installation meet the minimum hardware and software requirements. Your objectives for the MOM installation were discussed in Chapter 3. Those objectives determine how you will use MOM and that determines what components need to be installed.

Shortcuts…

Getting Started Again

As we discussed at the beginning of this chapter, even though you have already carefully planned your objectives for the installation of MOM 2005, there are a few things you should examine one more time before you begin the installation. Again, those things you should review include:

- The MOM 2005 Key Concepts
- Your deployment design and planning documents developed in Chapter 3
- The MOM 2005 release notes to identify any changes in the software that could affect your original plan
- The MOM 2005 Performance and Sizing Guide

Continued

- The MOM 2005 Security Guide
- The MOM 2005 Supported Configurations data sheet

You should go over these items one more time before you begin your installation on multiple computers so that any potential difficulties can be prevented if possible now.

As before, what components are going to be installed determine the minimum hardware and software requirements. It may seen somewhat redundant to go over these requirements again, but where we previously looked at the requirements for a single server hosting all components, we are now looking at multiple servers hosting individual components and the prerequisites are not quite so demanding.

It will also be of assistance to your installation to review the Microsoft Best Practices again.

Best Practices According to Microsoft

- Before installation, use the Performance and Sizing Guide located at http://go.microsoft.com/fwlink/?LinkId=46754 to assist you in determining what size your MOM database should be.
- Use a dedicated computer for the production MOM database.
- Install the MOM Database (EeaData.mdf) and log files (EeaLog.ldf) on separate hard drives for greater efficiency
- Install the SQL Server database and log files for MOM on a different hard drive than the paging file. The paging file usually is located on the same drive as the operating system.

The MOM Prerequisite Checker in MOM Setup can be used to verify the hardware and software prerequisites and to create a report listing those requirements that your installation destination meets or fails to meet.

The minimum hardware requirements to use the MOM 2004 SP1 Management Server are:

- A Pentium-compatible 550MHz processor or greater (dual Pentium-compatible 450MHz processors or greater recommended)
- 512 MB of RAM (1 GB or greater recommended)
- 5 GB of available hard drive space
- CD-ROM
- A network card

To install the MOM 2005 SP1 database, the minimum hardware requirements are:

- A Pentium-compatible 550MHz processor or greater (dual Pentium-compatible 450MHz processors or greater recommended)
- 512 MB of RAM (1 GB or greater recommended)
- 5 GB of available hard drive space
- A network card

To use the MOM 2005 SP1 Reporting Server, the minimum hardware requirements are:

- A Pentium-compatible 550MHz processor or greater (dual Pentium-compatible 450MHz processors or greater recommended)
- 512 MB of RAM (1 GB or greater recommended)
- 200 GB of available hard drive space to install Reporting Server and the initial reporting database
- A network card

A system that will host the MOM 2005 SP1 Administrator Console and Operator Console must meet these hardware minimum requirements:

- A Pentium-compatible 500MHz processor or greater (Pentium-compatible 1GHz processor or greater recommended)
- 128 MB of RAM (256 MB or greater recommended)
- 150 MB of available hard drive space
- Windows 2000-compatible video graphics adapter capable of displaying 1024x768 resolution with 24-bit color or greater recommended
- A network card
- A mouse or other pointing device

Some Independent Advice

As discussed before in this chapter, you should really make sure that you've verified the hardware and software of the target systems on which you want to install the various components. If the host machine does not meet the minimum requirements you should either remove that system from your deployment plan or upgrade the system so that it meets the minimum requirements.

Again, if the computer doesn't have the required software and hardware needed for an installation, you have two choices: either remove that machine from your deployment plans or upgrade the required hardware and install the required software so that it meets the required prerequisites.

Note

Remember, as we suggested earlier in the chapter when discussing installing all the components on one machine, the MOM 2005 Prerequisites can be rather picky during installation. You'll save yourself quite a bit of time by doing a clean install of the operating system and then immediately using Windows or Microsoft Update to make sure that all your operating system components are up to date.

Also as discussed earlier, another step you should complete before moving on to installing the various components is to verify the MOM 2005 Service accounts. Again, the three primary service accounts used by MOM 2005 are:

- The Data Access Server (DAS) Account
- The Management Server Action Account
- The Agent Action Account

These three accounts were discussed more fully earlier in the chapter and we will not repeat those explanations again here.

Best Practices According to Microsoft

It's recommended that different accounts be used for the MOM 2005 Management Server Action Account and the DAS account.

When you're installing MOM 2005 on multiple servers, as in this scenario, it's probably a good idea to divide the job into individual tasks to make sure that you get MOM 2005 installed correctly. There is a specific order by which MOM 2005 should be installed. That order contains seven phases and those phases are:

- Install the MOM 2005 database
- Install the first Management Server
- Install any additional Management Servers
- Discover Computers and deploy agents for first Management Server
- Discover Computers and deploy agents for additional Management Servers
- Install System Center Reporting
- Import Management Packs

Actually, installing System Center Reporting is an optional step that you can choose not to perform. This is the order, however, that the process should follow.

Let's start by discussing installing the MOM 2005 database. Before this step can be accomplished you must first install and configure SQL Server 2000 and SQL Server 2000 Service Pack 3a for the MOM 2005 database to use. You should also go ahead and make sure that all hotfixes for SQL Server 2000 with SP 3a are installed. If you're going to use an existing SQL Server, make sure that it meets these requirements and is configured correctly.

Three important things to remember about MOM 2005 and SQL Server 2000 SP 3a are:

- MSDE is not supported.
- There is a known issue that could arise when MOM 2005 bulk inserts data into the MOM 2005 database—the server process ID (SPID) may stop responding with a NETWORKIO (0x800) wait type and a constantly increasing wait time in SQL Server 2000 Enterprise Manager under Process Info or in the sysprocesses table in the master database. The only way to end the process is to kill the SPID. There's a hotfix available for this problem located at http://support.microsoft.com/default.aspx?scid=kb;en-us;884554.

- If your SQL Server configuration has both SQL Server 2000 and SQL Server 7 installed, you'll need to take a look at article number Q300341 in the Microsoft Knowledge Base.

As we have previously discussed the installation of SQL Server 2000 and the SQL Server 2000 Service Pack 3a earlier in this chapter, we won't belabor the point here again other than to briefly go over the important aspects of the installation. Remember that the SQL Server must be configured with these specifics:

- The database authentication should be set to Windows only.
- The SQL Server service account should be set to run as Local System. It can be set to run under a domain user account, and we discussed those reasons why you might want to do so during our previous discussion.
- The SQL Server should use TCP/IP sockets for all client connections.
- Make sure that both the MSSQLSERVER and SQLSERVERAGENT services are configured for automatic start when the system starts.

Installing the MOM Database on a Stand-Alone SQL Server

The first step in installing the MOM 2005 database on a stand-alone SQL Server after installing the SQL Server and SQL Server Service Pack 3a is to log into the computer where you want to install the MOM 2005 database using an account with administrator rights. This account must have DBO rights on the master and msdb databases on the SQL Server too. You need to close all open applications now because they could have an impact on the setup of the database.

Start the MOM 2005 installation by double-clicking the file setup.exe, which will load the Microsoft Operations Manager 2005 Setup Resources dialog window as shown in Figure 4.64.

Click **Install MOM 2005 Workgroup Edition** or **Install Microsoft Operations Manager 2005**, depending on which version you have. This will start the MOM 2005 Setup Wizard. Click **Next** on the Welcome dialog window and accept the license agreement as before and click **Next** again. Enter your username, organization, and the CD-Key; click **Next** again.

On the Installations Options dialog window, as seen in Figure 4.65, click **Custom**, and then **Next**.

Figure 4.64 The Operations Manager 2005 Setup Resources Dialog Window

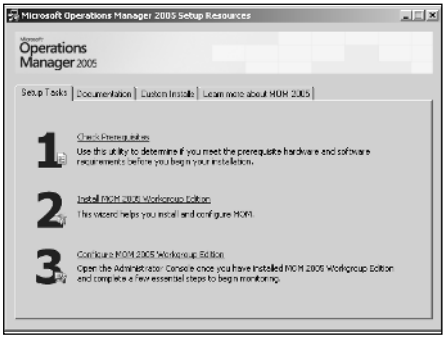
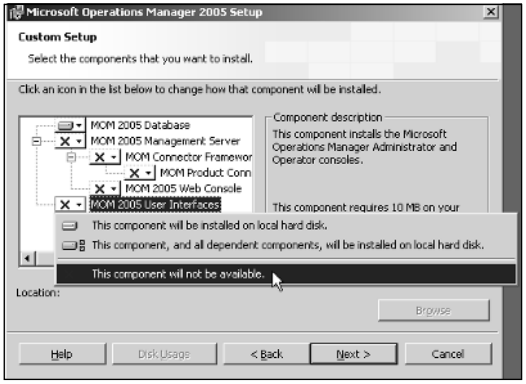


Figure 4.65 Click Custom Installation

On the Custom Setup dialog window, as seen in Figure 4.66, expand all components except for MOM 2005 Database, choose **This component will not be available**, and click **Next**.

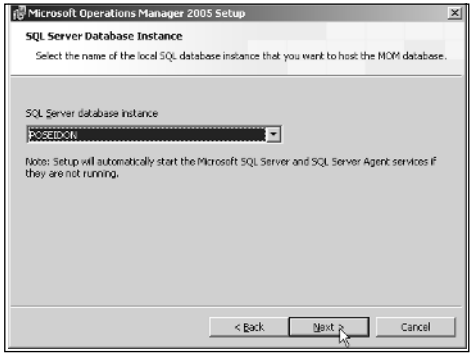
Figure 4.66 Make All Components except the MOM 2005 Database Unavailable



All prerequisites should have been met and you should be ready to begin the installation of the MOM 2005 components selected. If the prerequisites checker has failed, click the **View Log** button and determine what is causing the problem. Fix it, and run this wizard again. When all checks have passed, click **Next**.

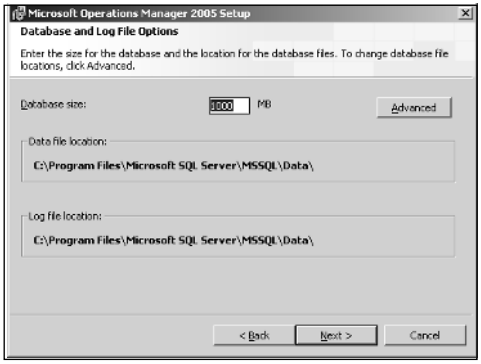
On the SQL Server Database Instance dialog window, as seen in Figure 4.67, choose the server instance in the SQL Server database instance drop-down list on which you want to install the MOM 2005 database. After you have made your selection, click **Next**.

Figure 4.67 Select the Database Instance You Want to Use



On the Database and Log File Options dialog window, as seen in Figure 4.68, adjust the size of the MOM 2005 database as discussed earlier in this chapter.

Figure 4.68 Adjust the Size and Locations of Your Data and Log Files



Some Independent Advice

Remember that we pointed out earlier that the MOM 2005 installation process installs the data file and log file on the same hard disk drive by default. You should change this setting to install them on different drives. We also strongly suggest that neither file be installed on the same disk as the operating system's paging file.

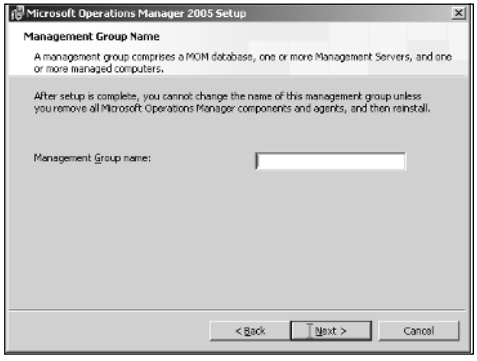
Remember also that the minimum and maximum supported size for the MOM 2005 database is 300 MB and 30 GB, respectively. A smaller size database will provide better performance so you should probably consider maintaining the database size between 12 and 15 GB.

Finally, as we pointed out earlier, the size of the log file is set to 20 percent of the size of the data file automatically by the MOM 2005 installation process. So if the data file is set to 10 GB then the log file size will automatically be set to 2 GB.

Click **Next** when you have finished adjusting the size and locations of these files.

The next dialog window, as seen in Figure 4.69, allows you to specify what name you want to use for this management group.

Figure 4.69 Choose the Name You Want to Use for the Management Group



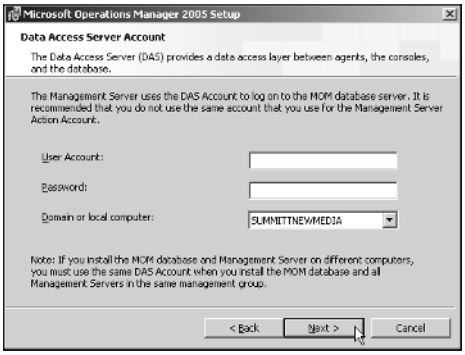
Best Practices According to Microsoft

The name you specify here represents the MOM 2005 database. It can be any name you choose consisting of alphanumeric characters, but each management group should be unique within your MOM 2005 environment. For a large system it would be advisable to use a naming convention to establish all management groups.

When you've named your Management Group, click **Next** to move on in the installation process.

As seen in Figure 4.70, enter the user account, password, and domain for the user account that you want to use to log into the MOM 2005 database server. You should not use the same account you used for the Management Server Action Account. Also, as in this scenario you are installing the MOM 2005 database and the MOM 2005 Management Server on different systems, so you must use the same account here that you use for any Management Server in the same management group. Click **Next** after you have entered the User Account, the Password, and the Domain or local computer.

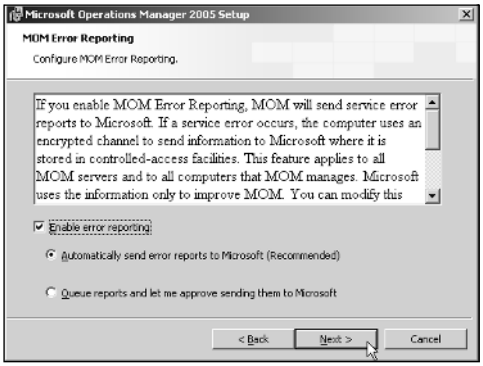
Figure 4.70 Enter the Account to Use to Log in to the MOM 2005 Database Server



As Figure 4.71 indicates, you now decide if you want to enable error reporting from MOM 2005 or not. As discussed previously, enabling error reporting sends an encrypted message to Microsoft containing information concerning the error. Check the option box to choose if you want to send these messages or leave it blank if you don't. You can also choose the **Queue error reports and let me approve sending them to Microsoft** option. This will cause MOM 2005 to store the error reports on the computer where they occur. The next time you log into that computer, a dialog box will appear and you will use it to send all the reports. When you have made your choice, click **Next**.

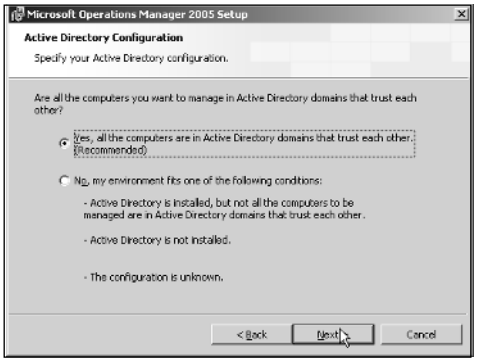
In our previous discussion of this section, when installing on a single computer, we explained that the Workgroup version and the standard version diverged at this point during the installation. If you are installing on multiple computers you should be using the Standard version and not the Workgroup version. The Standard version allows for the control of more computers and should be used in a scenario such as this; the Workgroup version handles smaller groups of computers and can easily be installed on a single computer.

Figure 4.71 Do You Want to Let Microsoft Know about Errors?



As Figure 4.72 indicates, choosing Yes is the default and recommend option. By choosing Yes you are stating that MOM 2005 can use mutual authentication for all communication between Management Servers and agents. If this is not the case, choose No. After making your choice, click **Next**. On the Ready to Install dialog window, click **Install**.

Figure 4.72 Are You Running Active Directory?



The installation of a new SQL Server database can take several minutes, depending on the size of the database specified. When it has completed click **Finish** to complete the process.

Installing and Configuring the First Management Server

So, we've performed all the steps required to install the MOM 2005 database. The next step is to install the first Management Server in our group. Installing the MOM

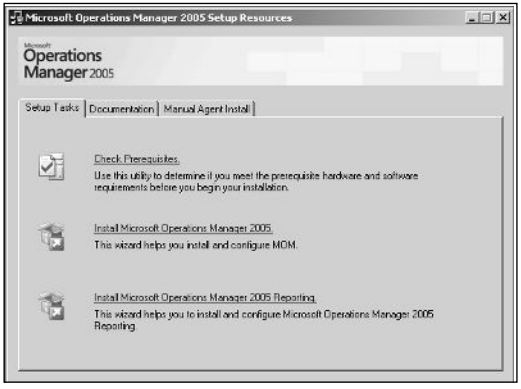
2005 Administrator Console and the MOM 2005 Operator Console on the same computer creates a Management Server.

Some Independent Advice

If you are going to create a MOM 2005 Management Server, you should probably set your screen resolution to 1024 by 768 with 24-bit color. This will enable the management screens to display properly.

To install your first Management Server, log on to the system you wish to install the Management Server on using an account with administrator privileges. This account should also have DBO access to the master and msdb databases on the MOM 2005 database server and db_owner access to the OnePoint database. Start the MOM 2005 installation process, and when the MOM 2005 Setup Resources dialog window appears, as seen in Figure 4.73, click **Install Microsoft Operations Manager 2005** to start the setup wizard.

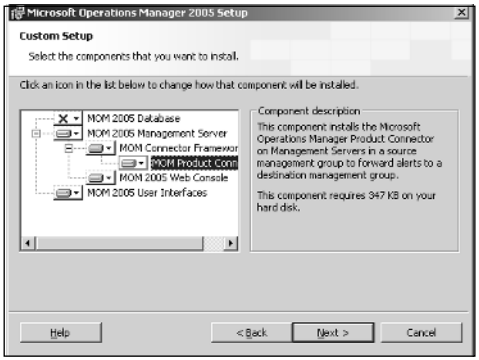
Figure 4.73 You Should Be Getting Very Familiar with This Screen by Now



When the MOM 2005 Setup Wizard starts, click **Next** on the Welcome dialog window. Accept the license agreement as before and click **Next** again. Enter your username, organization, and the CD-Key and click **Next** again. On the Installation Options page select **Custom** as when we created the MOM 2005 database.

On the Custom Setup Page, as shown in Figure 4.74, click **MOM 2005 database** and then click **This component will not be available**. All other options such as the MOM 2005 Management Server and the MOM 2005 User Interface should be changed to **This component will be installed on the local hard disk**. Click **Next**.

Figure 4.74 Change the Custom Setup Options as Shown



The Prerequisite check page will indicate if your system meets the requirements for a MOM 2005 Management Server or not. Continuing on the MOM Database Server Instance page you will type the SQL Server instance on which the MOM 2005 database was installed.

The next two dialog windows require you to provide the accounts you want to use for the Management Server and for the Data Access Server. Remember that these must be the same accounts that you used when installing the MOM 2005 Database. On the Ready to Install dialog window, click **Install**.

Installing and Configuring Additional Management Servers

You'll want to consider installing additional Management Servers to provide for agent failover. This allows for the possibility that if any Management Server should become unavailable, whatever the reason, any agents on its managed computers can report in to another Management Server in the same Management Group until their primary Management Server becomes available again.

Multiple Management computers will also allow you to distribute your managed computers and balance the workload within your MOM environment. You can install up to 10 additional Management Servers in addition to the First Management Server in the same management group. To install additional Management Servers in this management group follow the directions in the previous section.

Discovering Computers

The next two phases in the process of installing the MOM 2005 components on multiple machines are Discovering Computers and Deploying Agents for the First Management Server and Discovering Computers and Deploying Agents for

Additional Management Computers. But before you begin deploying those agents you should decide what computers you really want MOM 2005 to discover and manage.

Some Independent Advice

One of the first computers that you should consider putting an agent on is the system on which you installed your SQL Server and the MOM 2005 database. That way you'll be able to monitor the health and performance of one of the most important computers on your network, at least as far as the MOM 2005 framework is concerned.

Since we're installing more than one Management Server in the management group we need to decide which Management Server is the primary host for each of our managed computers next. Remember that MOM 2005 doesn't support software-based or hardware-based load balancing, so you'll need to balance the workload yourself by distributing your managed computers between the Management servers you have installed.

Shortcuts…

Discovering Computers in a Disjointed DNS Namespace

A disjointed DNS namespace is a DNS infrastructure that includes two or more top-level DNS domain names. The first step in discovering computers and installing agents using MOM 2005 in such a namespace is to use the MOM 2005 Agent Install/Uninstall wizard as described earlier in this chapter. Using the wizard, provide either a Domain\Computer name or a NetBIOS name format. Next, using the Create Computer Discovery Rule dialog, provide only the NetBIOS computer name or the Domain name and the NetBIOS computer name for the Domain Name and the Computer Name fields, respectively.

Keep in mind that some features will not be available. Those unavailable features include:

- Mutual Authentication
- Push install when using the Browse functionality for choosing the target computer

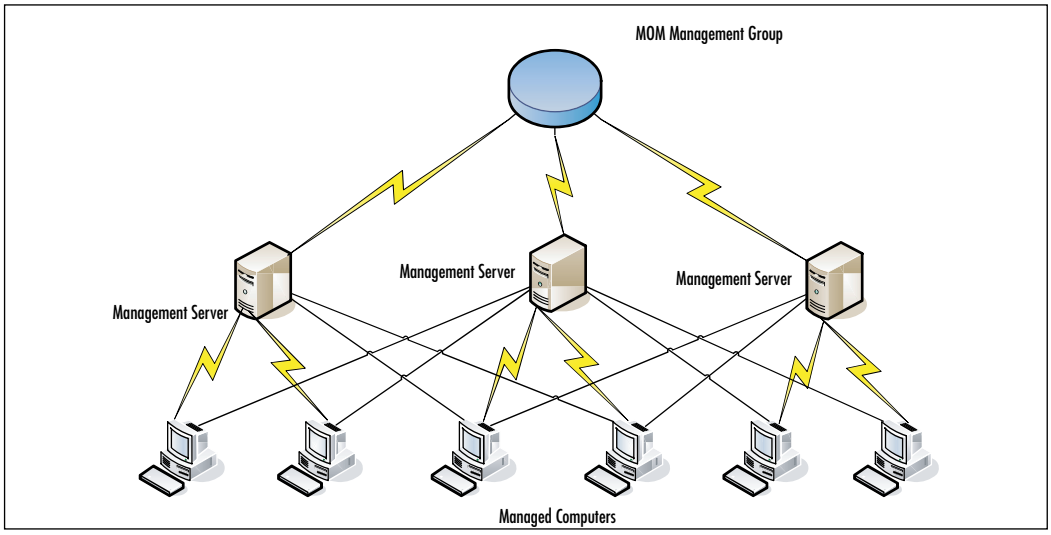
Continued

- Push install when using the DNS FQDN computer name

Mutual Authentication is supported if the Management Server being used is in a nondisjointed namespace and the supported computers and their agents are in a disjointed namespace.

In our example in Figure 4.75, we have one MOM 2005 Management Group, three Management Servers, and six managed computers. Each Management server is set as the primary Management Server for two managed computers. Should that Management Server fail, however, each managed computer can failover to one of the other Management Servers. This type of configuration helps to balance agent communication as well as response traffic with the Management Servers.

Figure 4.75 An Example Management Group



After you have discovered and deployed the agents for those computers you have designated as having the First Management Server as their primary using the methods we've already discussed, perform the same discover and deployment process for each of the Additional Management Servers in your Management Group. Keep in mind that the primary Management Server for a managed computer is the Management Server that you used to discover the computer and install the agent. Failover occurs when an agent cannot communicate with its primary Management Server. At that point in time it will automatically find another Management Server in the same Management group to communicate with. When you set up the additional Management Servers the process automatically configures each of them to serve as redundant Management Servers for the other Management Servers in the Management Group.

Installing MOM 2005 Reporting

The next phase in our installation of MOM 2005 onto multiple systems is to install MOM 2005 Reporting. This is actually an optional step in the installation process. The MOM 2005 Reporting Server includes the MOM 2005 Reporting Database and a scheduled job that periodically transfers data from the MOM 2005 database to the MOM 2005 Reporting Database. The MOM 2005 Reporting Console then makes it possible to run and view MOM 2005 reports that use data from the MOM 2005 Reporting Database using a supported browser.

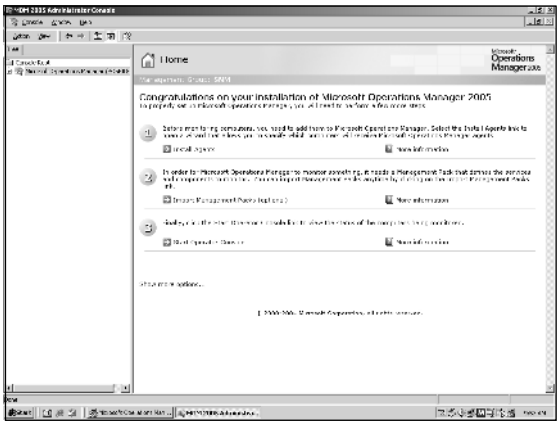
The installation process for MOM 2005 Reporting is basically the same for multiple systems as it was for the single system we already performed. The things to keep in mind here are that the MOM 2005 Reporting database and the MOM 2005 database can be on the same computer or on different computers. As with other factors previously discussed, the larger the management group and the number of systems being managed, the more likely you will get better performance from your systems if you install MOM 2005 Reporting on a dedicated system.

Deploying MOM 2005 Management Packs

The last phase of the installation of MOM 2005 onto multiple systems is that of importing MOM 2005 Management Packs. When you installed MOM 2005 the MOM Management Pack was installed automatically. Now that you've installed all the agents within your management group to MOM 2005, you're ready to import any other MOM 2005 Management Packs that you may want to use.

The first step to take for installing a management pack is to open the MOM 2005 Administrator Console and choose Import Management Packs, as seen in Figure 4.76.

Figure 4.76 Choose Import Management Packs



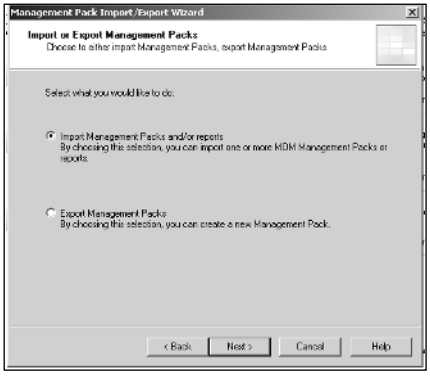
As with other aspects of the installation process discussed in this chapter, it is a good idea to develop a procedure that you will follow when importing Management Packs into your MOM 2005 Management group. The Welcome screen for the Import/Export wizard will appear. Click **Next**.

Best Practices According to Microsoft

Import any Management Packs you will be using into your test environment first and not directly into your production environment. This will allow you to learn how the Management Pack operates and what other configuration and permissions will be required for the Management Pack to perform correctly.

The default selection on the Import or Export Management Packs dialog window as seen in Figure 4.77 is to Import Management Packs and/or Reports. Accept the default and click **Next**.

Figure 4.77 Accept the Default and Click Next



On the Select a Folder and Choose Import Type dialog window as seen in Figure 4.78, click **Browse**.

In the Browse for Folder dialog window, as seen in Figure 4.79, navigate to the folder where the Management Pack is located and then click **OK**. When the dialog window disappears, click **Next** to continue.

Figure 4.78 What Type of Import Are You Performing?

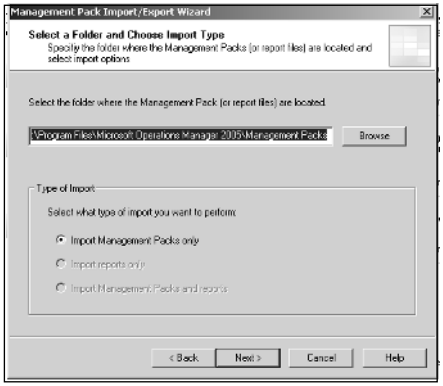
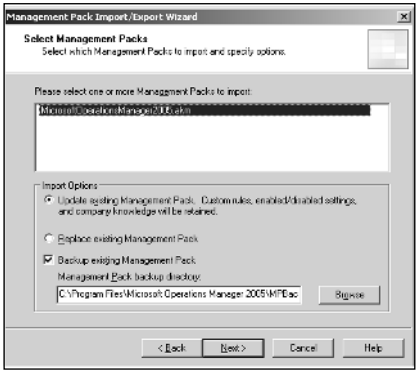


Figure 4.79 Navigate to the Location of the Management Packs

On the Select Management Packs dialog window, as seen in Figure 4.80, choose the Management Pack that you want installed, select an import option, and click **Next**. Click **Finish** to complete and close the wizard.

Figure 4.80 Choose the Management Pack You Wish to Install



After importing the Management Pack, the rules can be viewed immediately in the MOM Administrator console and the views can be viewed immediately in the MOM 2005 Operator Console.

Upgrading to MOM 2005

Upgrading from an earlier version of MOM can be easy or it can be complicated. It all depends on the size of your current MOM environment and the amount of planning you have put into your upgrade.

Understanding Upgrade Scenarios

If you've been using MOM 2000 SP1 and have all the components on a single computer it's a relatively simple and straightforward process to upgrade the system to MOM 2005. If the components are on multiple systems there is a specific order to upgrade due to interdependencies between the MOM components.

The upgrade process uninstalls the old components first and then the MOM 2005 components are installed in their place. The only exceptions to that are the MOM 2005 database and MOM Reporting.

SOME INDEPENDENT ADVICE

You can't upgrade to MOM 2005 Evaluation version from any previous version of MOM. This includes any previous version of MOM 2005. You will need to completely uninstall the previous version and then install MOM 2005

When you upgrade from the MOM 2005 Evaluation Edition you need to upgrade only the MOM database, Management Servers, and the consoles. Any agents installed, the MOM Reporting components, and the MOM Reporting database will not need updating.

Shortcuts…

Getting Started

As stated several times previously in this chapter, even though you carefully planned your objectives for the installation of MOM 2005 in Chapter 3, there are a few things you should go over one more time before you begin the installation. We repeat those things you should review again here:

- MOM 2005 Key Concepts
- Your deployment design and planning documents developed in Chapter 3
- MOM 2005 release notes to identify any changes in the software that could affect your original plan
- The MOM 2005 Performance and Sizing Guide
- The MOM 2005 Security Guide
- The MOM 2005 Supported Configurations data sheet

Another item that you should review would be the in-house documentation concerning the previous installation so as to insure that you have all the information required to perform the upgrade, such as account user names and passwords.

It's best to go over these items now before you begin your upgrade so that any potential difficulties may be overcome at this point in time.

Performing a Single Server Upgrade

Before we get into the discussion of the step-by-step procedure for performing a single server upgrade there are a few special considerations that need to be covered. If you have any computers running Windows NT 4.0 and you have MOM 2000 agents on these computers, you will need to remove them before you upgrade to MOM 2005. MOM 2005 does not support agents running on Windows NT 4.0. After the upgrade you can then discover these computers as agentless managed.

The next step before beginning the actual upgrade is to back up the MOM database. You should both back it up and verify that it can be restored before you proceed. The upgrade to the MOM 2005 database creates changes in the database structures and relationships. As a result, the upgrade can't be undone and can't be uninstalled. If you determine that you are going to need to restore the original

MOM 2000 SP1 configuration you will have to uninstall the MOM 2005 database components and delete the MOM 2005 database. Then you will be able to reinstall the MOM 2000 SP1 database component and restore the backup copy of the MOM 2000 SP1 database.

Shortcuts…

Backing up the MOM Database

First, open the Microsoft SQL Server Enterprise Manager and expand the Microsoft SQL Servers and its child nodes until the Management is displayed in the left pane of the window. Expand the Management node and right-click **Backup**. Next, click **Backup a Database**. In the SQL Server Backup dialog window, click the **General** tab and then click **OnePoint** in the database list. The Name for the backup will default to OnePoint backup. You can keep that name or change it as you wish. Click the **Options** tab and choose **Verify backup upon completion**. Click **OK** and the backup will begin.

You'll need to back up any ManualMC.txt files and any other files that you might have added to the MOM 2000 directory, too, because the setup process will delete them.

Now, simply run the MOM 2005 Setup on the single system you wish to upgrade to MOM 2005. There is nothing special you will need to do. The upgrade process is as simple as a normal single server install at this point.

Performing a Multiserver Upgrade

As with the single-server upgrade, before we get into the discussion of the step-by-step procedure for performing a multiserver upgrade there are a few special considerations that need to be covered. As with the single-server upgrade, if you have any computers running Windows NT 4.0 and you have MOM 2000 agents on these computers, you will need to perform the following:

- These computers can continue to be monitored up until the point where the agents must be upgraded.
- The upgraded management group for the agent on the Windows NT 4.0 computer must be removed.
- The Windows NT 4.0 computers may now be rediscovered from the upgraded MOM 2005 management group as agentless managed.

You should repeat the last two steps for each additional Management Server in your configuration group.

Shortcuts…

Removing the MOM 2000 SP1 Agent from a Configuration Group

The first step is to remove the agent computer. Next you need to perform a scan. You can wait for the next scheduled scan but it is better to perform it manually so that you can complete the process in a timely manner. After the scan, stop and restart the OnePoint service on the agent computer. You need to stop and restart because the registry of the agent will change as a result of the scan. The agent will not pick up that change, though, until the OnePoint service is restarted.

Again, as with the single server upgrade, the next step should be to back up the MOM database. Follow the instructions previously discussed. Also, any ManualMC.txt files and any other files that you might have added to the MOM 2000 directory will need to be backed up because they will be deleted as previously discussed.

For a Multiple System upgrade you need to follow a specific set of procedures in a specific order. That order is:

- The MOM Administrator Console installed on a separate computer
- The MOM database
- Management Servers
- Agents
- Reporting
- Management Packs

The actual steps involved are:

1. Upgrade the MOM Administrator Console.
2. Upgrade the MOM database.
3. Upgrade the First Management Server.
4. Upgrade the additional Management Servers.
5. Upgrade agents on Managed Computers.

6. Uninstall MOM 2000 SP1 Reporting and install MOM 2005 Reporting.
7. Import any MOM 2005 Management Packs.

Let's look at each step individually. If you have any stand-alone MOM Administrator consoles in your MOM environment, you'll need to run the MOM 2005 Setup on that system to upgrade the MOM Administrator console component. Remember that the MOM Administrator Console must be closed before you begin the upgrade and that if you have the Web Console installed, you need to uninstall both consoles before you start the upgrade process.

If a console is installed on a computer that also hosts the MOM database or a Management Server, the setup process will upgrade the console at the same time as when you upgrade the database or the Management Server. The process will uninstall the MOM 2000 SP1 Administrator console and replace it with the MOM 2005 Administrator Console and the MOM 2005 Operator Console.

During this upgrade process you'll be asked for the name of the Management Server to which you want the MOM 2005 Administrator Console and the MOM 2005 Operator Console to connect. Enter the name of your First Management Server.

The next step is to upgrade the MOM database. Remember that during this process the database will be upgraded to the MOM 2005 version and cannot be uninstalled. Again, back up the original database and test the restore before you begin this process.

If you have a MOM 2000 SP1 agent on the system that is hosting the MOM database, uninstall the agent before you begin the database upgrade process. Run the MOM 2005 Setup on the system hosting the database after performing the preceding steps. You'll be prompted to provide the DAS account name and password. This must be the same DAS account as that used for MOM 2000 SP1 or any Management Servers that have not yet been upgraded will not be able to communicate with the upgraded MOM 2005 database.

Don't upgrade the agents that report to the First Management Server until all Management Servers have been upgraded. Also, when you upgrade the First Management Server, the MOM 2005 Management Pack is installed by default. Don't import any other MOM 2005 Management Packs until all other Management Servers and agent computers have been upgraded. If you do you'll see erroneous alerts and events to the nonupgraded Management Servers by any multihomed agents.

Upgrade the First Management Server using the same process discussed previously, then use the same procedures to upgrade any additional Management Servers.

After all Management Servers within your environment have been upgraded, and only after all have been upgraded, you can begin to upgrade the agents within your environment. You can upgrade these agents in any order and the MOM 2005 Management Pack will be deployed automatically to the upgraded agents.

Some Independent Advice

A word about mutual authentication at this point: This option provides for greater security on your network by requiring the Management Server and the agents to authenticate with one another before communicating. This requires a two-way Active Directory trust relationship between the Management Server and the managed computers.

This option is turned off by default during an upgrade and you shouldn't enable it or change the port used for communication with the agents until all agents in your environment have been upgraded to MOM 2005. Changing these settings prior to that will cause loss of communication with all nonupgraded systems.

You'll next need to upgrade MOM Reporting. Remember that MOM 2000 SP1 Reporting cannot be upgraded to MOM 2005 Reporting. As a result you need to uninstall MOM 2000 SP1 Reporting and install MOM 2005 Reporting as a clean install. You can install it on the same computer as SQL Server Reporting Services or they can be installed on separate computers.

Best Practices According to Microsoft

While you can install Reporting on the same computer as the MOM database or a Management Server, for optimum performance, you should install the MOM Reporting console on a dedicated computer.

Finally, the last step in the upgrade process is to import any MOM 2005 Management packs. Remember, make sure that you've upgraded all MOM agents before you import the Management Packs.

Some Independent Advice

It's a good idea to import only one Management Pack at a time. This will give you the opportunity to evaluate the effects of the Management Pack on your environment and tune the Management Pack to stabilize the data that is generated.

Performing a Side-by-Side Upgrade

It can take a long time to upgrade your MOM components in a large enterprise environment. As a result, you might want to consider using a side-by-side upgrade. Here, you would deploy a totally new MOM 2005 management group right along side the preexisting MOM 2000 SP1 environment. You might also consider using this type of upgrade if you have specialized configuration groups in your environment.

Using the side-by-side upgrade allows you to use multihomed MOM 2005 agents that belong to both MOM 2000 SP1 configuration groups and MOM 2005 Management groups. That means that you can gradually deploy the new MOM 2005 agents to managed computers while continuing to monitor those computers not upgraded in the MOM 2000 SP1 configuration group.

Advanced Scenarios

The last part of this chapter looks at installing and deploying MOM 2005 in advanced environments. These environments would include clustered servers, multiple domains, beyond firewalls, and installations using the command line. As we close out this chapter we will look specifically at clusters and command line tools.

As with the previous sections of this chapter, your first step should be to make sure that the systems you are planning to use meet the minimum hardware and software requirements listed in the MOM 2005 Supported Configurations document. This document, named SuppConfig.htm, is available in the RelDocs directory on the MOM 2005 CD. It is also available online.

Deploying on a SQL Cluster

MOM 2005 supports the installation of the MOM database on a SQL Server cluster for failover purposes only. Only the MOM 2005 database components, the MOM 2005 agent, and the MOM 2005 Reporting database and components can be installed on a SQL Server cluster. No other components can be installed on the cluster.

If you are updating a database on a cluster, upgrade the primary, or active, node first leaving the passive node box on the setup dialog window unchecked. Then make the next node active and check the passive node box on the setup dialog window. Repeat this step for each of the remaining nodes in the cluster.

Deploying the Database

If you are deploying the MOM 2005 database on an active cluster for the first time, run the MOM 2005 database creation tool (momcreatedb.exe) locally on the

computer where the SQL Server instance is active. Make sure that the MOM database and log files reside on a hard disk owned by the SQL Server cluster group. Repeating this process on all SQL Server instances will install the database on the multiple nodes. The process is very similar to the process performed before in this chapter.

Deploying Reporting

Again, the process of deploying reporting and the reporting database on a SQL Server Cluster is very similar to the process of deploying the MOM database on a SQL Server Cluster. Again, you can deploy the MOM Reporting Database on only one SQL Server node at a time.

You must perform a full installation on the first node and then only a partial on the subsequent nodes. You can install the MOM Reporting Database only on an Active node, so each node must be made active before you start the installation. After the first installation you must select the Passive Node of a Windows Server Cluster checkbox to signify that the node will be configured as a passive node.

Using the Command Line to Deploy MOM 2005

In the land of GUI it is good to know that you can still deploy MOM 2005 from the command line. You can deploy all the MOM 2005 components including agents and MOM reporting using this interface.

As long as you have local administration rights on the target computer you can use MOMAgent.MSI, MOMServer.MSI, and MOMReporting.MSI with their various command line options to install MOM 2005 components on one or more computers. For example, the following syntax would install an agent with a control level of Full installed in the default location using an account other than the default local system account for the MOM Agent Action Account:

```
Msiexec /i \\<location of setup program>\MOMAgent.msi
CONFIG_GROUP=”group_name”
MANAGEMENT_SERVER="server_name" AM_CONTROL="Full" ACTIONSUSER="account_name"
ACTIONSPASSWORD="account_password" ACTIONSDOMAIN="domain_name" /q
```

The following syntax would be used to install the Administrator and Operator consoles:

```
Msiexec /i CDdrive\MOMServer.msi ADDLOCAL="MOMXUI"
MOM_Server="ManagementServerComputerName" /q
```

The Microsoft Operations Manager 2005 Deployment Guide provides extensive details concerning further syntax examples and details explanations of each command-line option.

Summary

In this chapter we have looked at a variety of scenarios dealing with the installation of the various versions of MOM 2005. Specifically we have covered:

- Verifying MOM 2005 prerequisites
- Installing SQL Server 2000 and SQL Server 2000 Service Pack 3.0a
- Installing SQL Server 2000 Reporting Services
- Installing MOM 2005 Standard and Workgroup Edition on a Single Server
- Installing MOM 2005 Service Pack 1
- Installing MOM 2005 Reporting
- Performing a multiserver upgrade
- Performing a side-by-side upgrade
- Deploying an SQL cluster
- Using the command line to deploy MOM 2005

Second only to planning, proper installation is one of the most important factors on which your MOM 2005 installation's success depends. This chapter has dealt with some specifics, but mostly has offered you options to consider in your installation process. You know your environment. You know your needs. Take the information we've provided and make it yours as you plan and install your MOM 2005 environment.

Solutions Fast Track

Installing on a Single MOM Server

- ☑ Verify that your target system meets all MOM 2005 minimum requirements
- ☑ Install the server components required
- ☑ Install and prepare SQL Server 2000, SQL Server 2000 SP 3.0a , and SQL Server 2000 Reporting Services
- ☑ Install the MOM 2005 components
- ☑ Install the MOM 2005 Reporting Service
- ☑ Discover computers

Installing on Multiple MOM Servers

- ☑ Verify that your target system meets all MOM 2005 minimum requirements
- ☑ Install the MOM 2005 database on a stand-alone SQL Server
- ☑ Install and configure the first management server
- ☑ Install and configure any additional Management Servers
- ☑ Installing the MOM 2005 Reporting Service
- ☑ Discover computers

Upgrading to MOM 2005

- ☑ Verify that your target system meets all MOM 2005 minimum requirements
- ☑ Perform a single-server upgrade
- ☑ Perform a multiserver upgrade
- ☑ Perform a side-by-side upgrade

Advanced Scenarios

- ☑ Deploy the MOM 2005 database on a SQL Server cluster
- ☑ Deploy the MOM 2005 Reporting database on a SQL Server cluster
- ☑ Deploy MOM 2005 using the command line interface

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: What is MOM 2005 Workgroup Edition?

A: The MOM 2005 Workgroup Edition originally was known as MOM Express.. The Workgroup Edition is a limited version of MOM 2005 that is aimed at managing 10 or fewer servers. It includes only a subset of the full MOM 2005 functionality, but is fully capable of handling the needs of most small to medium businesses.

Q: Will the evaluation version of MOM 2005 upgrade to MOM 2005?

A: Before the evaluation version expires to MOM 2005. The migration process will allow you to maintain all the information you stored during your evaluation of the product.

Q: Can I use a different database with the evaluation version of MOM 2005 if I don't have Microsoft SQL Server?

A: Unfortunately, SQL Server 2000 is the only database that will work with MOM 2005 at the time of this writing. Microsoft says that they will fully support SQL Server 2005 but they are currently still in the testing phase. You can get the evaluation version of SQL Server from Microsoft at www.microsoft.com/downloads/details.aspx?FamilyID=D20BA6E1-F44C-4781-A6BB-F60E02DC1335&displaylang=en. MOM 2005 does not support Microsoft SQL Server Desktop Engine, Access, or any non-Microsoft database product.

Q: Can I upgrade my existing MOM 2000 environment to MOM 2005?

A: The upgrade process from MOM 2000 SP1 to MOM 2005 is a smooth, easy, in-place migration.

Q: What are MOM 2005 management packs?

A: MOM 2005 management packs provide built-in, product-specific operation information and rules for a wide variety of your server applications. They contain rules for monitoring a wide variety of server health indicators and can create alerts, often before a problem arises, when situations are detected or reasonable thresholds are exceeded that may require administrator intervention. This capability is sup-

ported by in-depth knowledge base content, prescriptive guidance, and actionable tasks that can be associated directly with the relevant alerts included in the management packs. You can then take actions to prevent or correct situations, such as degraded performance or service interruption, maintaining service availability with greater ease and reliability.

Q: Are any management packs included with MOM 2005?

A: The following management packs are included in MOM 2005:

- Microsoft Baseline Security Analyzer
- Microsoft Exchange 2000 Server
- Microsoft Exchange Server 2003
- Microsoft Operations Manager 2005
- Microsoft SMS 2003
- Microsoft SQL Server 2000
- Microsoft Windows Active Directory
- Microsoft Windows Base Operating System
- Microsoft Windows DNS
- Microsoft Windows IIS
- Microsoft Windows Server Clusters

You can also obtain these management packs from the Management Pack Catalog. In addition, remember that all MOM 2000 management packs will continue to work with MOM 2005.

Q: Can I use my MOM 2000 management packs with MOM 2005?

A: Any management pack running on your MOM 2000 SP1 system will be migrated to MOM 2005 during the upgrade process. The new management packs provided with MOM 2005, however, provide additional information, such as topology and state views, as well as reporting. Any custom changes or modifications you may have made to your MOM 2000 management packs will be carried forward when that management pack is used in an upgraded MOM 2005 environment.

Q: Are the management packs and rules that I developed maintained when I upgrade from MOM 2000 SP1 to MOM 2005?

A: As stated in the previous question, after these management packs have been migrated to MOM 2005, you will have access to all the changes and rules that you have made in the past as well as being able to add new functionality, such as topology and state views and custom reporting.

Chapter 5

Understanding and Deploying Management Packs

Solutions in this chapter:

- **Defining a Management Pack**
- **Working with Management Packs**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

Management packs are the heart of MOM 2005 and provide the rules that allow you to monitor and collect information across multiple systems in your environment. There are numerous management packs available for MOM 2005 from both Microsoft and third-party partners and vendors, but don't overlook the ability to create your own management pack. In this chapter we will look at the definition of a management pack, followed by a look at a number of the management packs provided by Microsoft and third-party partners. We will then look at the tools available to create your own management packs to monitor your own line of business applications.

Defining a Management Pack

At this point in the book you should be well aware of what MOM 2005 is designed to do and you should also have a strong understanding of the three key phases that MOM addresses when dealing with server issues including identifying potential issues and problems on your monitored systems, understanding the specific details of the problem, and providing automated resolution to the problem when applicable. All three of these key phases are driven by the management packs imported and configured within MOM 2005.

At its simplest, a management pack (MP) is a collection of rules and possibly accompanying reports that provide a set of criteria used by MOM agents to help determine what information to collect, act on, and forward to the MOM management server. Rules within a management pack are divided into three types: event rules, alert rules, and performance rules. Management packs also often include other components in addition to rules such as tasks, and views that are specific to the management pack. All these components can be created by any member of the MOM authors group and exported as an .akm file, the file association used with management packs or an .xml file in the case of reports.

Digging a little deeper into the key elements of a management pack you will find the following:

- **Alerts** As the name implies, alerts are intended to call attention to critical events that require either administrator intervention or automated resolution. Rules within a management pack are defined to generate alerts based on a specific set of defined criteria about a specific event and help to define the health of your monitored systems.

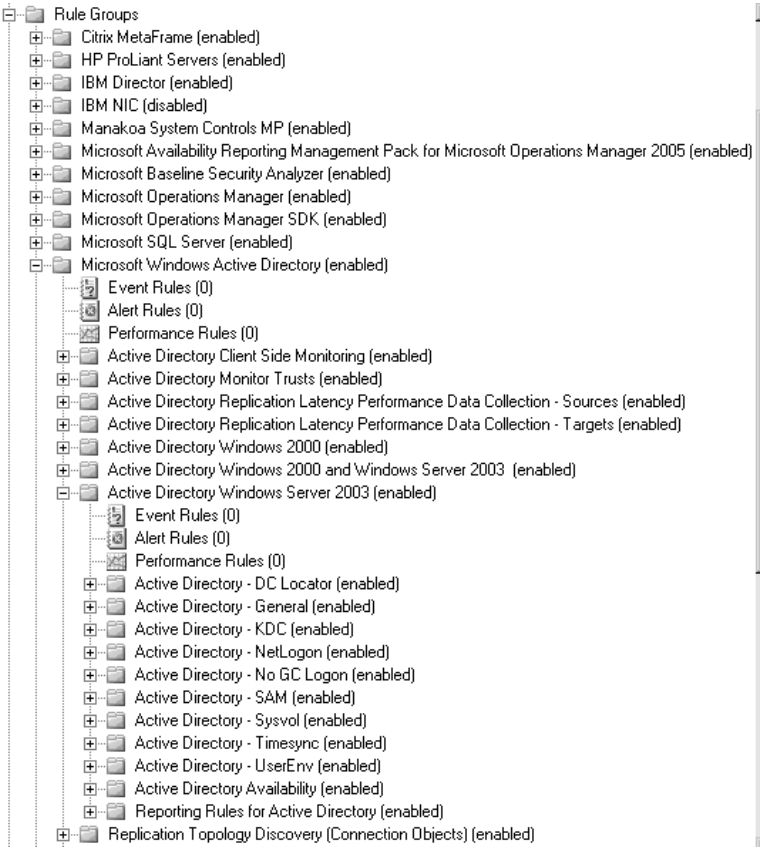
- **Product Knowledge** Most (not all) of the rules contained in management packs released by Microsoft contain a section called Product Knowledge, which provides guidance and built-in expertise for individual rules, helping to guide administrators in resolving outstanding issues.
- **State Monitoring** State monitoring is new to MOM 2005 and provides an at-a-glance view of the state of your monitored systems including the health of the operating system and the applications, and is organized by the role of each server. Examples of server roles include Exchange, AD, and SQL. State monitoring further breaks down the health of each component of the operating system and application. For example, the operating system is broken down in disk, memory, and CPU components.
- **Views** Views provide a targeted look based on defined criteria into the health of a server and allow MOM operators to investigate specific health indicators, including performance data. Views allow you to focus on a specific collection of events or alerts for all monitored systems or targeted to specific groups of monitored systems.
- **Tasks** Tasks enable MOM operators to respond to events and alerts from within the Operator console by providing access to tools, utilities, and MMC snap-in in the Tasks pane. Tasks help to improve the overall efficiency of an operator when responding to an event or an alert by allowing an operator to launch the required administration tool from within the Operator console. Custom tasks can be defined by the management pack author to further automate the sometimes common steps used to diagnose and resolve issues on monitored systems.
- **Reports** Reports provide you with the ability to run ad hoc reports or define subscriptions to reports based upon user-defined criteria to allow for historical data analysis and to better understand long-term trends in operational and application performance.

How Management Packs Work

Management packs generally are organized into a hierarchical structure, defined by folders but referred to as rule groups (RGs), that allows you to logically organize rules based on a specific version of an application or specific functionality within that application or operating system component. Take the Active Directory MP as an example; within the MP shown in Figure 5.1, you can see that the parent directory is called Microsoft Windows Active Directory and the child rule groups (folders) below this parent include:

- Active Directory Client Side Monitoring
- Active Directory Monitor Trusts
- Active Directory Replication Latency Performance Data Collection—Sources
- Active Directory Replication Latency Performance Data Collection—Targets
- Active Directory Windows 2000
- Active Directory Windows 2000 and Windows Server 2003
- Active Directory Windows Server 2003
- Replication Topology Discovery (Connection Objects)
- Replication Topology Discovery (Site Links)

Figure 5.1 Logical Organization of ADMP



As you can see from Figure 5.1, the Microsoft Windows Active Directory MP is further broken down into rule groups specific to Windows 2000 Active Directory and Windows Server 2003 Active Directory. Although these logical groupings provide easier navigation and administration, the key reason for this structure is to allow for associations between rule groups and computer groups to be made. To better understand this, look at Figure 5.2, which again shows the ADMP but this time highlights the parent rule group named Microsoft Windows Active Directory. In Figure 5.2, pay particular attention to the right pane, known as the display pane, and the Bound to Computer Groups: None section. It is not uncommon to find that the parent container is not bound directly to any computer groups. The logic behind this is that more granular computer group bindings can be defined at lower levels in the rule group hierarchy.

Figure 5.2 Rule Group to Computer Group Binding

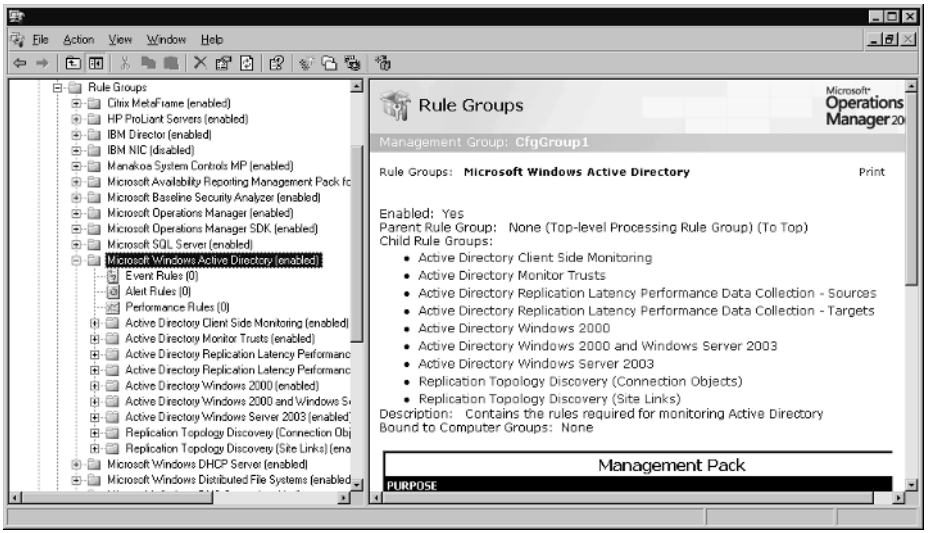
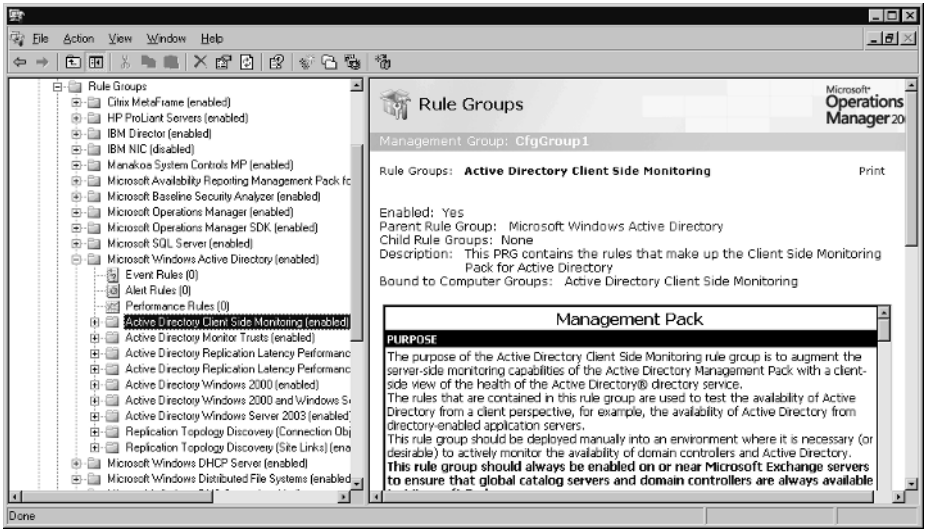


Figure 5.3 shows one of these lower level bindings. Here you can see that we have changed our focus in the Administrator console by selecting a child rule group named Active Directory Client Side Monitoring. If you look at the display pane again, specifically to the *Bound to Computer Groups* section, this time you will notice that this rule group is bound to the Active Directory Client Side Monitoring computer group. This binding means that all the rules in the Active Directory Client Side Monitoring rule group will be received by the monitored agents that are members of the Active Directory Client Side Monitoring computer group. Membership in computer groups is determined by the computer attributes that are found on a monitored system during a computer attribute discovery.

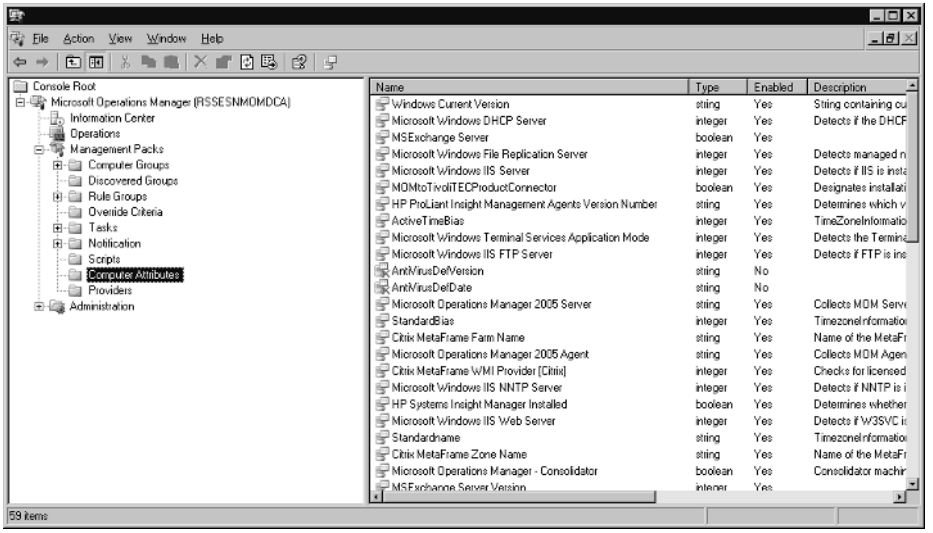
Figure 5.3 AD Client Side Monitoring Computer Group Binding



NOTE

The MOM agent performs attribute discovery locally in an attempt to determine the roles defined on the monitored system, and forwards the resultant information on to the MOM Management Server. For example, computer attributes define the role of Domain Controller, the version of the operating system, such as Windows Server 2003, or the role of an Exchange Front-End Server. Computer attributes often are included in MPs but can also be created manually after a MP is imported using the Administrator console, in the Management Packs node as displayed in Figure 5.4. Computer attributes are specific keys or values within the registry that help to determine the roles running on a monitored system.

Figure 5.4 Computer Attributes



So the first step in creating your own custom management pack in the Administrator console is to create a parent rule group. This can be accomplished by right-clicking on Rule Groups in the Administrator console, selecting Create Rule Group, and entering the name of the rule group. I often like to create a group called Custom Rules – Company Name for the customers that I work with as a consultant, and following best practices, not link this to any computer groups. Then within that parent rule group, I create one or more child rule groups for each of the different customized rules I create. It is at this child rule group level that I begin binding computer groups to the appropriate rule groups.

Best Practices from Microsoft

Should you ever want to modify anything within a default rule included in a management pack that you have imported, right-click on that rule and select copy. Then paste that rule either into the appropriate child rule group in your custom rule group or paste a copy of that rule into the original location. Then disable the original rule and make your modifications to the copied version. The reason for this is that every rule is identified by MOM 2005 by its GUID, and by copying and pasting the original rule, you are creating a new rule with a new GUID. This becomes increasingly important when an update to the management pack becomes available and you decide to upgrade to the newer version. If you simply had modified the built-in rule, it's very likely that the modifi-

cations that you made would be overwritten by the identical rule included in the updated MP.

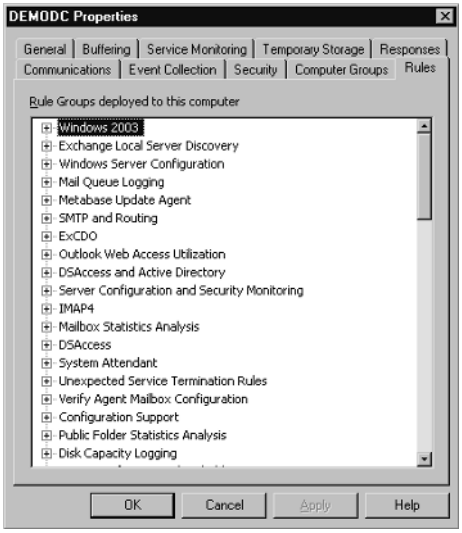
When copying rules, it is also important to understand that the knowledge contained within the original rule on the Knowledge tab does NOT copy to the new rule by default. You can change this default behavior by right-clicking on Rules Groups in the Administrator console and enabling Author mode. Author mode will add an additional tab to the properties of your rules called Knowledge Authoring, and will allow you to define the knowledge sections and text within each section, or to share knowledge between two rules and then regenerate the knowledge for all rules in the rule group and populate that once empty Knowledge tab. In the end, it is up to you to ensure that the rules you create contain knowledge.

The next obvious question is usually, "how can I determine what's changed from the version I am using to the new version?" The answer to that can be found in a number of tools, some of which will be discussed later in this chapter. One tool available to assist you with this is a MOM 2005 Resource Kit utility known as MPDiff and the other is a third-party tool from Silect Software (www.silect.com), known as MP Studio Express.

Another question that tends to come up when discussing the principle of binding rule groups to computer groups is, "how do I determine what rules an agent is receiving?" Like most things Microsoft, there is usually more than one way to get the result you are interested in and this holds true when determining the rules that are being received by a specific agent.

To view the rule groups that are bound to a specific agent, open the Administrator console and navigate to the Administration node, expand Computers, and select Agent-managed Computers. Double-click on any computer and the Properties dialog box of that system will appear, allowing you to select the Rules tab, where as you will see in Figure 5.5, all the rule groups that are currently being received by that monitored agent are displayed.

Figure 5.5 Displaying the Rule Groups Applied at a Monitored Agent

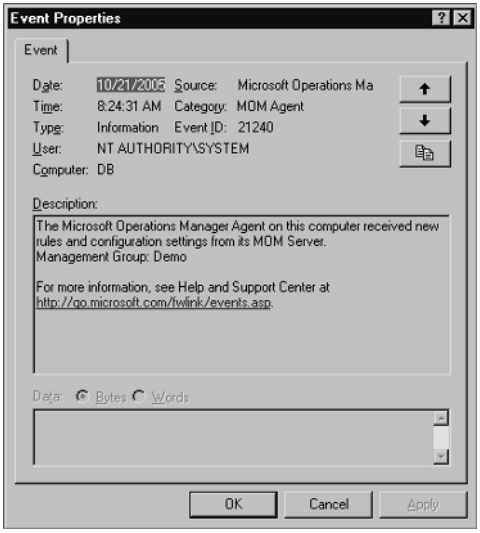


Another way to view this information at a more granular level is to use the MOM 2005 Resource Kit Tool, Resultant Set of Rules (rsor.exe). The command line options and syntax for this command are very simple: just type *rsor.exe MOMDB MOMAgent*, where MOMDB is the name (NetBIOS or FQDN) of the MOM database server and where MOMAgent is the name of the monitored agent that you wish to identify which rules have been deployed.

Best Practices from Microsoft

When you make changes to rules in the Administrator console, it is recommended that immediately following that rule change, you right-click on the Management Packs node and select Commit Configuration Changes. This commits the changes made through the Administrator console to the OnePoint database and helps to ensure that those changes are not lost. Once rule changes have been committed, agents will obtain those rule changes at their next configuration polling interval (every five minutes by default). If you are interested in knowing if rule changes have been received on a monitored computer, look at the Application log for Event ID 21240 from source Microsoft Operations Manager as shown in Figure 5.6.

Figure 5.6 Event ID 21240 Confirming Rules Changes Have Been Received



Within a management pack, as you saw earlier in Figure 5.3, there are three different types of rules: event, alert, and performance rules. Let's take a look at the differences between each of these, and at the subtypes within the respective rule types.

Event Rules

Event rules allow you to define how MOM (agent or server, as they can run on both) responds to events from a variety of providers. Some of the more common providers include the built-in event logs such as Application, System, and Security, and in the case of servers configured with DNS or Active Directory, the DNS and Directory Services event logs. Other providers include the WMI, timed event, or log file providers that allow you to event on WMI queries, run scripts to generate events based on a MOM administrator defined schedule, or pull information out of application-specific event logs.

There are five different types of event rules available to you in MOM 2005, and these include:

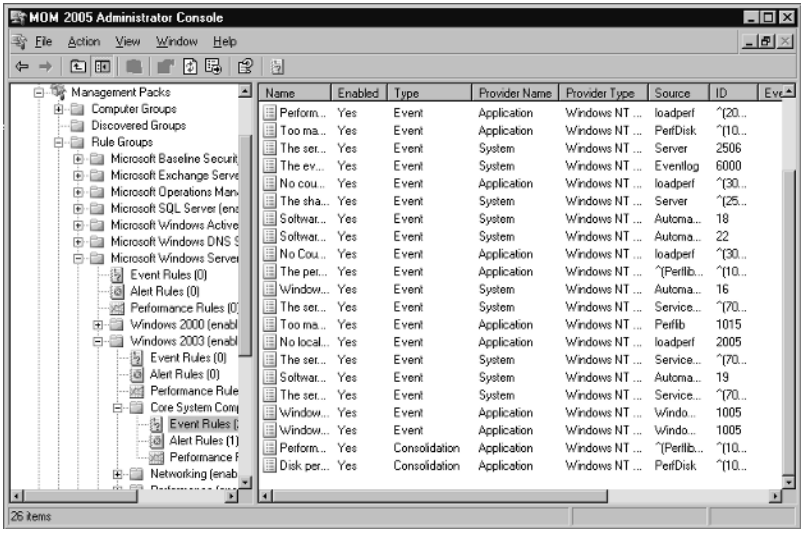
- Alert on or Respond to Event (Event)
- Filter Event (Pre-Filter)
- Detect Missing Event (Missing)
- Consolidate Similar Events (Consolidation)
- Collect Specific Events (Collection)

Let's take a look at each of these event rule types in more detail.

Alert on or Respond to Event (Event)

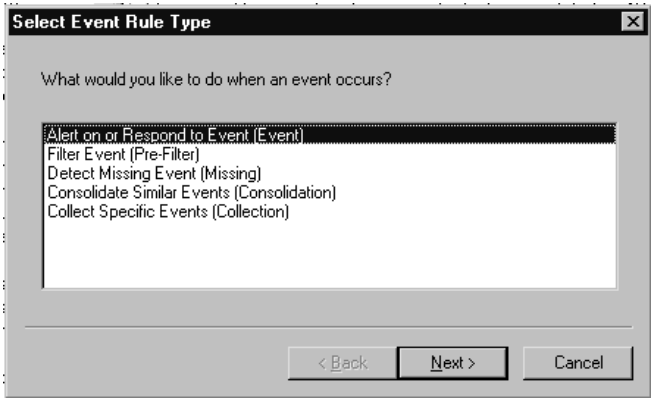
This event rule allows you to instruct MOM to generate an alert or run a response when a specific event occurs that meets a set of criteria that you are able to define. If you are interested in configuring an event rule to alert you when certain expected events are received, this too is possible and is covered later under the Detect Missing Event rule type. Figure 5.7 displays a listing of the different event rule types found in the Microsoft Windows Servers Base Operating System | Windows 2003 | Core System Components and Services rule group. Pay particular attention in Figure 5.7 to the Type column in the display pane, which in this example shows that two types of event rules are being utilized in this rule group, event and consolidation rules. Event rules, the short form of the event rule type, Alert on or Respond to Event.

Figure 5.7 Rule Types in the Core System Components and Services Rule Group



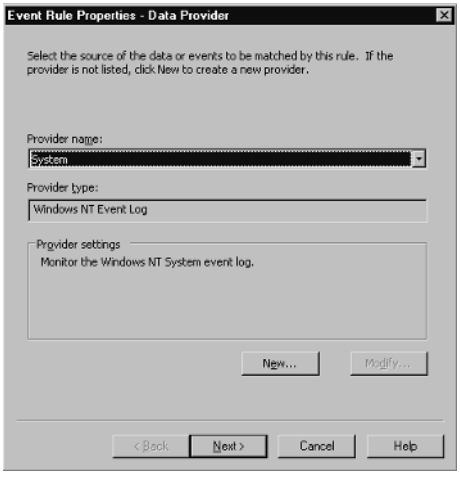
Creating an Alert on or Respond to Event rule is quite easy. Within the Administrator console, expand the Management Pack node, expand Rule Groups and navigate to the rule group in which you wish to create the new rule, expand that rule group folder and right-click on Event Rules, and select either Create Event Rule or the specific type of event rule you wish to create from the context menu. Should you elect to choose Create Event Rule, the first dialog box you are presented with will ask you to choose the event rule type you wish to create, as displayed in Figure 5.8.

Figure 5.8 Creating an Alert on or Respond to Event Rule



The next selection you will be asked to make, assuming you select the Alert on or Respond to Event (Event) rule type, is to select a provider. Note that the options will change depending on the rule type you elect to create. To show you an example of a rule that I usually create for customers that use SNMP internally, let's select the System event log provider on the Data Provider page shown in Figure 5.9.

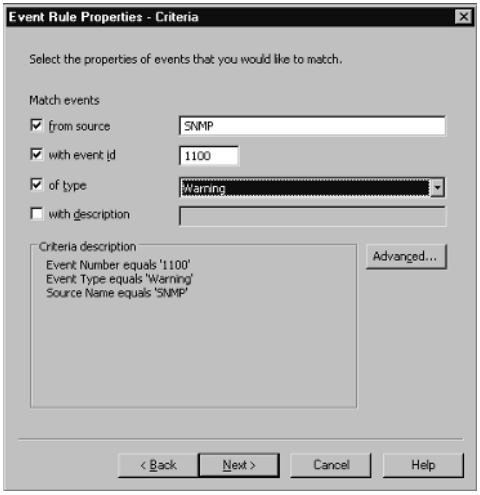
Figure 5.9 Selecting a Data Provider



Next you will be asked to choose the criteria that the event will match. As you can see from Figure 5.10, you have the ability define the source, event id, type, and description that the event will have. If this isn't enough, you also have the ability to select Advanced and define even more criteria and use Boolean or regular expressions. In this example, we will select **from source** and enter **SNMP** and **with**

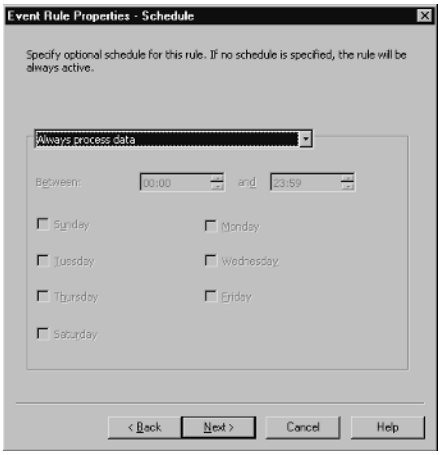
event id and enter **1100** as well as **of type** and select **Warning**. This rule will alert us to SNMP configuration issues that log a warning in the system event log with event ID 1100.

Figure 5.10 Defining Event Criteria



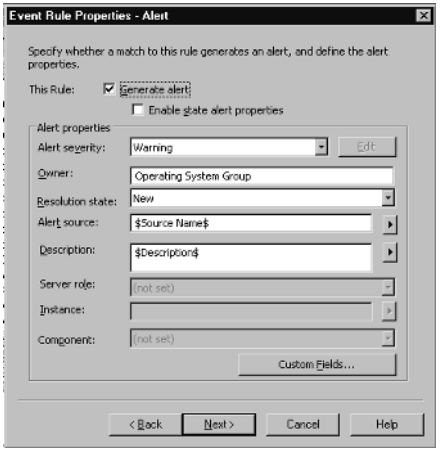
On the schedule dialog box shown in Figure 5.11, you have the ability to define the schedule under which the rule will be active. The default, as you can see from Figure 5.11, is to always process the data; however, this feature allows you the ability to make the rule active only during a specific period. An example of this might be a rule that is used to look for a specific event that you know within your environment occurs daily between the hours of 04:00 and 06:00. If you know this to be the case, and the event fires only during this time period, there is no need to have the rule active 24 hours a day.

Figure 5.11 Setting the Event Schedule



With all this information defined, you are now asked if you wish for the event to generate an alert. Events do not have to generate alerts, but to see them in the Alerts view in the Operator console, you will have to enable the Generate Alert option (see Figure 5.12). When the Generate Alert option is enabled, you have the option of specifying the alert severity associated with the event. Here you have a range of options from Success through Service Unavailable. In our example, we will configure the SNMP event to generate an event and set the alert severity to Warning. Normally, I don't generate an alert but for the purposes of this example, I will enable it. Instead of creating an alert, I normally create a custom Event View in the Operator console that looks for and displays these events to me so that I can take the appropriate action from within the Operator console.

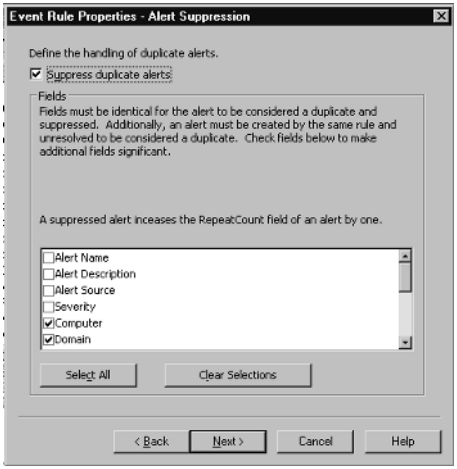
Figure 5.12 Generating an Alert



In a large enterprise environment, you can also specify an owner for the event. An example of this is where you have a group that is responsible for the support of the operating system and another group responsible for Exchange. Because this event, related to SNMP, would fall under the jurisdiction of the operating system group, an individual or the name of the group could be entered as the owner. This provides you with more filtering options when creating Alert responses that we will talk about later in this chapter in the section dedicated to Alert rules. You are also able to define the resolution state that you want the alert to have when it is generated. The default alert resolution state is New, but you can change this to any one of the other options or define your own customer alert resolution state for monitoring and tracking.

Next in the Alert Suppression dialog box shown in Figure 5.13, you will see the option to suppress duplicate alerts enabled. Leaving this enabled is a good best practice because it will help you to avoid alert storms. Alert storms are large volumes of alerts often generated by an incorrectly configured rule or an improperly configured application that is producing a large number of events that are being monitored and alerted on by MOM. With alert suppression enabled, when five similar or identical events occur that are configured to generate alerts, a single alert will be generated as opposed to five individual alerts, and the RepeatCount variable stored within the one alert that is generated will be incremented five times. This way, you can easily identify rules that are firing repeatedly and generating alerts without being overwhelmed by identical alerts in the Operator console. This feature within MOM allows the amount of noise within your environment to be suppressed so that the operators are able to see the most critical events and alerts as opposed to being overwhelmed by everything that's going on within their environment. This is one of the key reasons why tuning the rules in your MPs and defining thresholds that are relevant to your environment is so important.

Figure 5.13 Alert Suppression

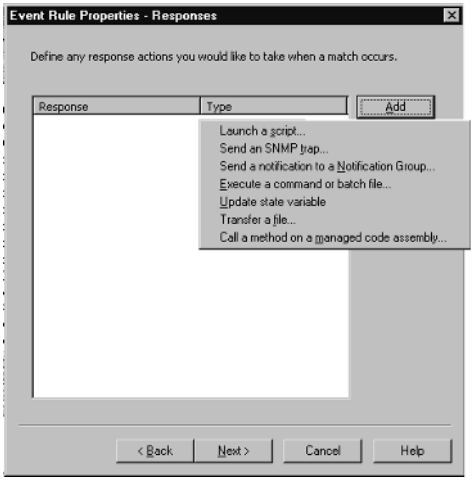


In the Responses dialog box shown in Figure 5.14 you have the ability to define one or more responses to the event rule. The response options available to you include:

- Launch a script
- Send an SNMP trap
- Send a notification to a notification group
- Execute a command or batch file
- Update a state variable
- Transfer a file
- Call a method on a managed code assembly

If, based on this event occurring, you wanted to be alerted, you would select the Send a notification to a notification group response, which would allow you to select a notification group from the list of available notification groups. Once a notification group was selected, you can then decide on the type or types of notification formats you want to utilize. Your options here include sending an e-mail, a page, or specifying a specific command format. If the built-in notification options aren't enough to meet your organization's sophisticated needs, you can look to the Notification Workflow solution accelerator available at www.microsoft.com.

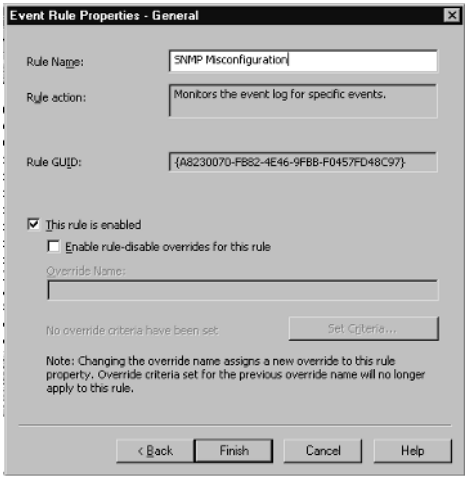
Figure 5.14 Event Responses



Once you have configured the responses that you are interested in, you have the ability to add company-specific knowledge to the rule. This can be very beneficial within medium and large organizations to help reduce the amount of time spent solving repetitious issues within your environment by allowing you to document and capture the steps taken to resolve the problem. These steps can then be referenced in the future and more junior support personnel can use this information to resolve these types of known issues, helping to extend your return on investment.

The last thing that you need to do prior to finishing the creation of your new rule is to give it a name in the General dialog box. The name of this rule is SNMP Misconfiguration, as displayed in Figure 5.15.

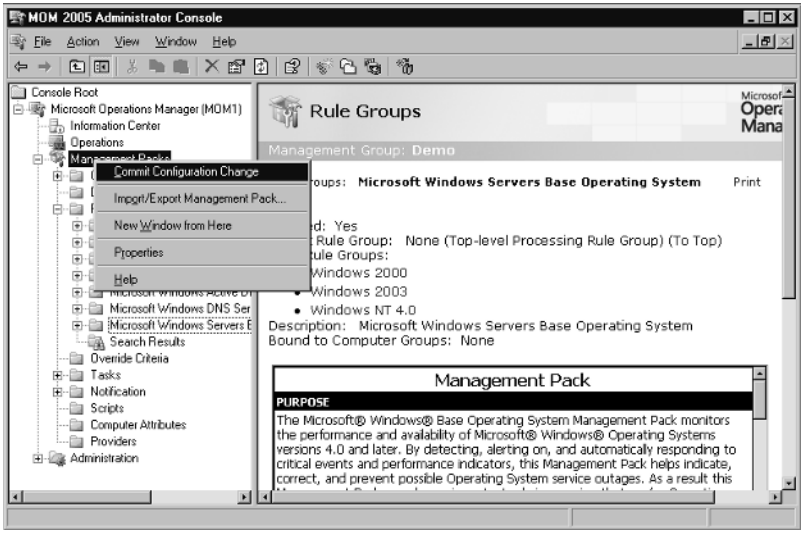
Figure 5.15 General Rule Properties



Another important feature, and one that is new to MOM 2005, can be seen in the General dialog box shown in Figure 5.15—that is rule overrides. Rule overrides allow you to configure a rule and then disable the rule for specific computers or computer groups. The benefit of this feature with event rules is that if you have a computer that is in production and being monitored, and you are experimenting with some settings (SNMP, for example, in the case of the rule you just created), then you can set a rule override to disable this event rule from applying to that one computer or to an entire computer group so that it won't generate events or alerts based on the events triggered on that one system.

Now that you are done configuring the rule, it's very important that you commit the changes. This can be done by right-clicking on the Management Packs node in the Administrator console and selecting **Commit Configuration Change**, as shown in Figure 5.16.

Figure 5.16 Committing Configuration Changes



Filter Event (Pre-Filter)

Pre-filter event rules allow you to specify events that you wish to ignore. These are typically events that are enumerated but that you don't consider significant within your environment. Examples of these types of events might be successful print job events.

Detect Missing Event (Missing)

The missing event rule, as the name implies, allows you to create a rule that looks for a specific event and generates an alert or response if that event isn't generated during a specified time. One example of this might be a rule to monitor for the successful completion of your nightly backup. If you know that your backup application writes to the application log, and this normally occurs between 01:00 and 05:00, you could create an event rule to notify you if an information message isn't logged to the application log, indicating that your backup successfully completed during that time period.

Consolidate Similar Events (Consolidation)

The consolidation event rule allows you to group multiple similar events into a single summary event on an agent monitored system, and then forward only a single event to the MOM management server.

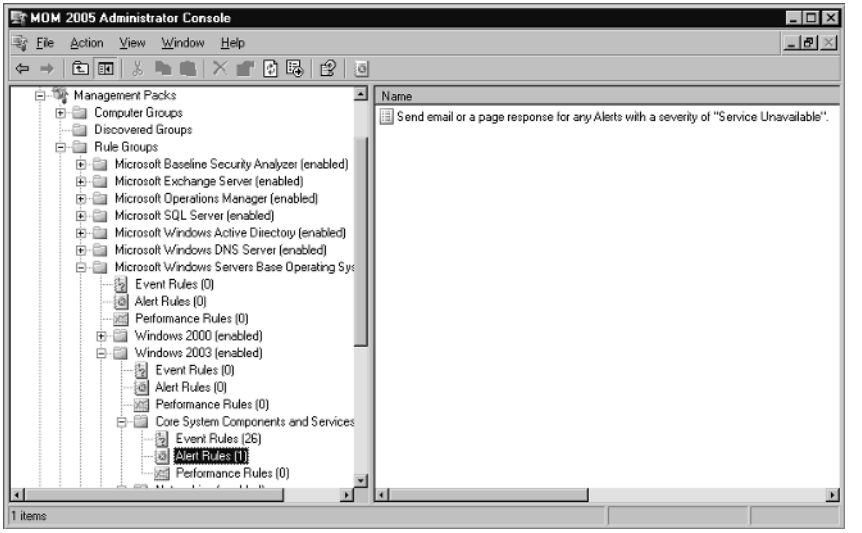
Collect Specific Events (Collection)

Collection events allow you to create rules that collect data from events with specific criteria that you are able to define. Unlike other types of event rules, collection rules do not allow you to configure responses or generate alerts. Collection rules can be useful in helping you collect specific information for long-term trend analysis and reporting.

Alert Rules

Alert rules allow you to create a single rule that based on specific criteria in an alert, and generate a response for all rules that meet that defined criteria. For example when discussing Event rules, you learned that a notification response can be defined for each individual Event rule that you create. Although this is possible, it may not be the most efficient use of your MOM operator's or administrator's time. Instead, a single Alert rule can be created that looks for specific criteria such as the severity level of an alert, and generates a response for all alerts with the specified severity level. This is the way that Microsoft writes their management packs as you can see in Figure 5.17, which shows the properties of the Alert rule in the Microsoft Windows Servers Base Operating System | Windows 2003 | Core System Components and Services rule group, where only a single Alert rule exists. Pay particular attention to the display pane and the name of the Alert rule shown in Figure 5.17. As you can see by its name, Send email or a page response for any Alerts with a severity of "Service Unavailable", this rule will send a notification based on the severity information in one or more event rules.

Figure 5.17 Alert Rules



Performance Rules

There are two types of performance rules, measuring rules and threshold rules, both of which use performance monitor counters to collect and report on the performance of your monitored systems. Performance rules allow you to define how MOM processes performance counter data on one or more monitored systems.

Measuring Rules

Measuring rules are included to allow you to define rules that collect performance-related information for long-term trend analysis, reporting, and forecasting.

Threshold Rules

Threshold rules, as the name implies, are included to allow you to monitor against specific performance thresholds and trigger alerts when the thresholds you define are exceeded, allowing you to be notified when performance is degrading.

Now that you have an understanding of the rule types and subtypes found within a management pack, let's take a look at the type of functionality that is available in third-party MPs.

Third-Party Management Packs

Microsoft has gone to great lengths to try to have a management pack created for all their various operating systems and applications, and have been quite successful to

this end for applications and operating systems that they develop. Their vision, however, does not include creating management packs for third-party software and operating systems. They have left the filling of this void up to third-party vendors to supply management packs for non-Microsoft applications. Although this did get off to a slow start, significant momentum has been achieved since the release of MOM 2005 in August 2004, and numerous vendors now provide management packs for non-Microsoft applications and operating systems.

To learn more about the growing list of management packs from both Microsoft and third parties, look at the management pack catalog at www.microsoft.com/mom.

Some examples of the types of applications and operating systems that you are able to monitor with MOM 2005 include server hardware from Dell and HP using MPs, available for free from these OEMs. The use of these OEM MPs is covered is greater detail in Chapter 9. Network devices such as Check Point, Nortel devices, and even storage devices from EMC can be monitored through virtual agents provided by eXc Software (www.excsoftware.com). Other network devices from Cisco such as routers, switches, and PIX Firewalls can be monitored using MPs from Jalasoft (www.jalasoft.com). Non-Microsoft operating systems such as Linux, AIX, and different flavors of UNIX can also be monitored using third-party management packs; this is covered in greater detail in Chapter 10.

Agentless Management

Earlier in Chapter 3 we looked at the three different monitored computer types, and it's worth revisiting one of those three—agentless monitoring—when talking about management packs because there are a number of limitations and requirements that you need to be aware of.

Agentless monitoring provides you with the ability to monitor remote resources (computers and other devices) without the requirement of installing an agent. These systems are monitored in a way that is similar to how local resources are monitored on agent-monitored systems and leverage multiple providers and responses in the management of these devices. Assuming the provider you wish to use supports remote access to resources and the responses you wish to use can execute their logic remotely, then the rules work the same way on both agentless and agent-monitored computers. The name agentless monitoring, however, is a bit of a misnomer because an agent is installed, but it's installed just on the MOM management server as opposed to the agent being monitored. Hence all monitoring is conducted from the MOM management server across the network using remote procedure calls (RPCs) to the device or computer in question. Once identified, MOM starts monitoring the agentless computer as though there were an agent installed on the computer. One of the require-

ments for agentless monitoring is that the MOM Action account must have administrative user rights on the computers you wish to manage agentlessly.

A lot of the functionality that works on agent-managed systems will also work on agentless managed systems with a few exceptions. What is not available to you through agentless monitoring is support for application log providers. Limitations with script and command-line responses used in timed events must leverage the new $TargetComputer$ property in order to access the agentless server. Lastly, the descriptions of event log entries on the agentless machine are not displayed on the MOM management server unless it has the same EventLogmessages.dll file as the agentless computer. What this really means is that if your MOM management server is running on Windows Server 2003 and an agentless managed computer is running Windows NT 4.0 Server then you will not receive the descriptions of event log entries collected on the Windows NT 4.0 Server. A workaround to this issue is to install the software for which you'd like to receive event log entries on the MOM management server.

Other issues that should be taken into account when considering agentless monitoring is that it will not work through a firewall in typical configurations, because agentless network traffic uses remote procedure call (RPC) and Distributed Component Object Model (DCOM), which in turn use ports that aren't often open on most firewalls. Some management packs will not work in agentless mode; some examples include the Active Directory and the IIS management packs. Look to the management pack configuration guides for agentless monitoring support information.

Working with Management Packs

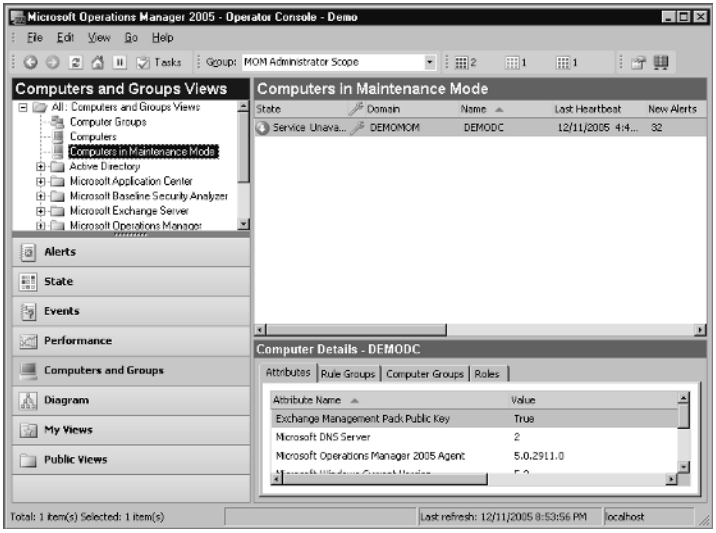
Earlier in this chapter you learned about the different rule types available in MOM 2005. Other important components of MPs include Views, Tasks, and Providers, so in this section you will learn about each of these additional components of a management pack. We won't cover reporting in this section simply because it is covered for each of the management packs covered in later chapters.

Let's begin with a look at Views and learn how we can create custom views that allow us to monitor for events or alerts that meet specific, administrator-defined criteria. Views, although a part of a management pack, are one of the few components that are defined in the MOM Operator console as opposed to the Administrator console.

Views provide you with a window into the events and alerts being collected by your MOM agents and forwarded up to the MOM management server. One of the most common View requests I receive from clients is to be able to view all the systems that are currently in maintenance mode, so let's take a look at how to create a

computer view to see this. In the Operator console select **Computer and Groups** and right-click **All: Computer and Groups View**, select **New**, and select **Computer View**. In this view we want to view all computers that satisfy specified criteria, so select computers that satisfy specified criteria. Next, scroll down to the bottom on the criteria dialog box and enable in Maintenance mode, and then give the view a name such as **Computers in Maintenance Mode**. Now, you have your custom view, as you can see in Figure 5.18. Also take note of the icon that denotes Maintenance mode, a wrench that appears to the left of the Domain column when looking at the default view in the Operator console.

Figure 5.18 Custom Views



SOME INDEPENDENT ADVICE

After placing a computer in maintenance mode, it's a good idea to wait up to 10 minutes before making changes, stopping and starting services, or recycling the server altogether since it can take that long for the Maintenance mode change to be reflected on the monitored agent. When a computer is in Maintenance mode, events are still received but alerts are suppressed to prevent erroneous responses such as notifications from being sent out when server maintenance is being performed.

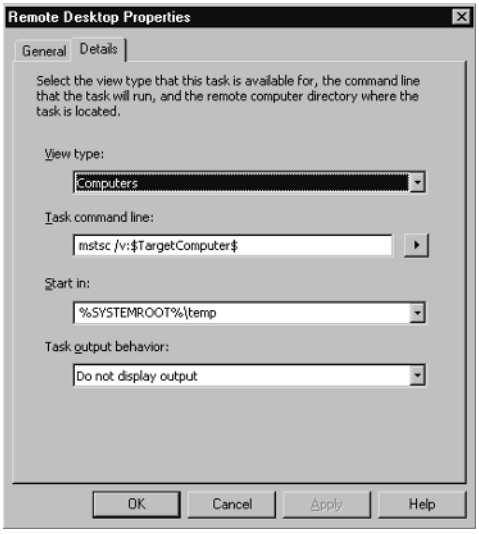
Now that you are familiar with how to create a new view, let's take a look at how you can create custom tasks in the Administrator console that will then be

available to you in the Operator console. New tasks can be created within the Management Pack node in the Administrator Console by right-clicking **Tasks** and selecting **Create Task**. There are two types of tasks available to you in MOM 2005: console tasks and runtime tasks.

Console Tasks

Console tasks, as the name implies, run in the Operator console and execute on the same computer on which the Operator console is installed. Console tasks can be launched in the context of the users selection, allowing the user to pass the name of the selected computer as a parameter to provide context as to how the task should be run. Console tasks run in the security context of the user that is running the Operator console. Console tasks can be only command-line tasks, meaning that the action that is executed is specified in terms of a command line to execute. When a task gets launched against the selected item in the Operator console, the properties of the item can be passed to the command line as parameters. For example, if we look at the properties of the Remote Desktop task as shown in Figure 5.19, you will see that the command line to execute this task is **mstsc.exe /v:$TargetComputer$**. Here, the variable $TargetComputer$ will be replaced by the computer name of the selected item in the Operator console. Tasks defined for the computer view type are available for computers, alerts, and events. When defining a console task the commands should start with an executable file name (.exe, .bat, .wsf, .js, .vbs, .cmd, etc.) including the extension, and then command line parameters can be included after the filename.

Figure 5.19 Task Properties



The set of relevant and available attributes that can be passed into the command line as parameters will vary, depending on the view type selected. In the Alerts view type for example, the Alert Name of the selected alert can be passed as a parameter.

To create a new task that launches the services.msc, start by right-clicking **Tasks** in the Administrator console and select **Create Task**. Leave the default **Operator Console** selected as the run location and the task type as **Command line**. In the View type drop-down dialog box, select **Computers** and in the Task command line type **services.msc –s /computer:$ComputerName$.** Change the Start in path to **%windir%\system32** and select **Do not display output**. Give the task a name such as **services** and test the newly defined task in the Operator console. You may have to refresh the console (CTRL + F5) to see the new task.

Runtime Tasks

Runtime tasks can be executed either on a management server or on an agent-managed computer. You have more options available to you with runtime tasks than you do with console tasks in that you can select from multiple task types including Command line, Script, Managed Code, and File Transfer tasks. With a runtime task you also are able to specify what type of entity the task is designed for, and this information is used by the Operator console to present instances of the class as possible task targets when the user is launching the task.

The task target role controls two things. First, it controls which attributes are available for passing into the command as parameters and second, it controls which targets the task can be launched against. For example, if a task is defined for the SQL role and the user tries to launch the task against a computer that does not have that role, the Run Task Wizard will fail. Additionally, if the computer on which the user has selected to run the task hosts more than one instance of the target role, the user can select which instance(s) to run the task on and the task will be run once for each selected target role instance.

Runtime tasks always run in the security context of the Action Account, and it is not possible to substitute the security context (i.e., Run As) when running a runtime task. Only members of the MOM Authors and MOM Administrators groups can execute runtime tasks.

Providers

The last management pack component that we will look at is Providers, which are a key component of a rule. Providers determine how and where to get the data that rules depend on. MOM exposes the following provider types that give management

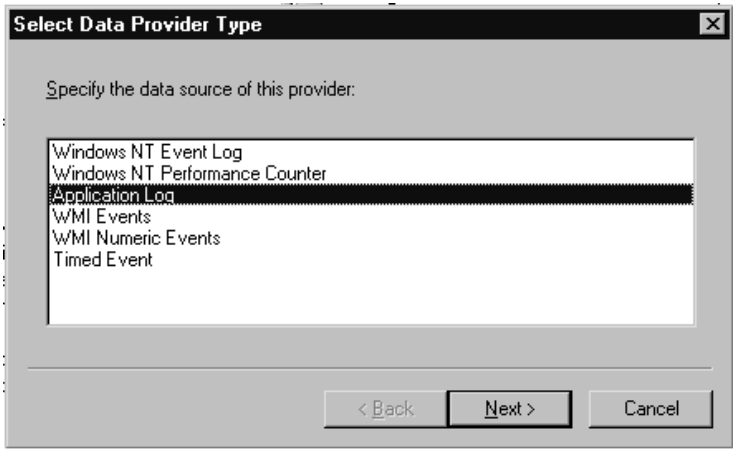
pack authors access to many of the most commonly used data sources for monitoring and management:

- Windows NT Event Log Provider
- Windows NT Performance Counter Provider
- Application Log Provider
- WMI Events Provider
- WMI Numeric Events Provider
- Timed Event Provider

MOM also provides the ability to create custom providers to allow MOM operators to collect data from data sources, such as custom Windows NT Event Logs or a Performance Counter objects without writing any code.

One example of a rule that can be created to use a custom provider is a rule that I often create for customers to look for Active Directory clients that are connecting from IP addresses not associated with any AD sites. This triggers a system event from source Netlogon with event id 5807, and also writes the offending client information to a log file named netlogon.log on a domain controller. To create a rule to collect the information written to this log file, we will first have to create a new provider. This can be done by right-clicking **Providers** in the Management Pack node in the Administrator console and selecting **Create Provider**. Here you will have a number of options as you can see in Figure 5.20; we will select **Application Log**.

Figure 5.20 Creating a Provider



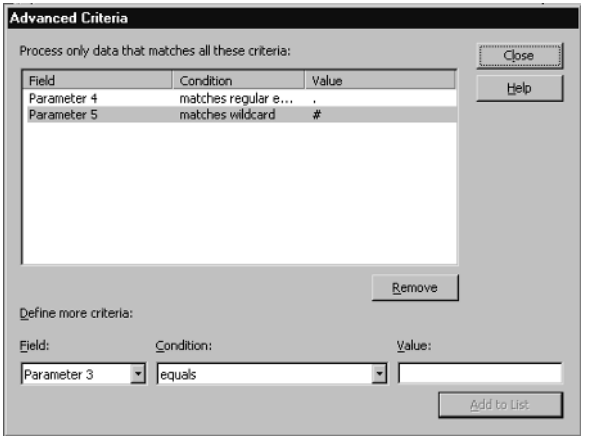
In the Provider name, type **Netlogon**, and in the Provider log type drop-down list, select **Generic Single-line log file**. In the Directory Edit dialog box type **%Systemroot%\debug** in the **Directory** text box and select **Generic** in the Format drop-down menu. Click **Add** as shown in Figure 5.21.

Figure 5.21 Directory Edit

In the File Pattern section of the Directory Edit dialog box shown in Figure 5.21, type **netlogon.log**. Now that the new provider has been created, you can create a new event collection rule that collects events logged in the %Systemroot%\debug\netlogon.log file.

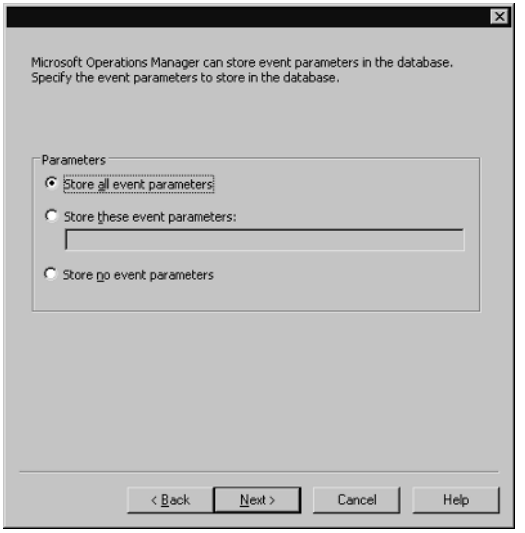
To do this, open the Administrator Console and expand the Management Packs node. Create the new rule in the Microsoft Windows Active Directory, Active Directory Windows 2000 and Windows Server 2003, Active Directory—Netlogon rule group by right-clicking **Event Rules** and selecting **Collect Specific Events**. In the Provider name drop-down box, select **Netlogon** and on the Criteria tab, click **Advanced**. In the Field drop-down menu, select **Parameter 4** and select **matches regular expression** in the Condition drop-down menu. Type **.** in the Value text box and click **Add to List**, as shown in Figure 5.22. Then in the Field drop-down menu, select **Parameter 5** and select **matches wildcard** in the Condition drop-down menu. Type **#** in the Value text box followed by **Add to List**.

Figure 5.22 Defining Advanced Criteria



Select **Store all event parameters** in the Parameter Storage dialog box shown in Figure 5.23.

Figure 5.23 Parameter Storage



Continue through the remainder of the dialog boxes accepting the defaults, give the new rule a name, and click **Finish**. You have now created a new collection rule that uses your new provider.

Acquiring Management Packs

The first source I always check for management packs, both Microsoft and third party, is the management pack catalog at www.microsoft.com/mom. This is an ever-growing list of available management packs for all supported MOM versions. It goes without saying that the way in which the management packs are listed and the usability functionality on the page could be improved dramatically, as you can see in Figure 5.19. My understanding is that the MOM Product Group is working on this so we'll have to wait to see what happens. What would be nice is the ability to sort alphabetically or by RTM date. Even nicer would be the ability to simply connect to the Microsoft Update site from your MOM management server and have it run a scan of the MPs installed, and return to you a list of updates for what is installed, and a list of what isn't installed that you might want to consider importing. It would also be really nice if there was a report that displayed all installed management packs and their version information, but that would require the creation of a custom report at this time.

Microsoft tends to release all their management packs as .msi files so as a general rule, after downloading these, I usually recommend to clients that they extract these to a specific folder on a network share and restrict the permissions to that folder share to allow only MOM Administrators access. Within this folder, I also often recommend that an Excel spreadsheet be included that lists the name of the MP.msi, the friendly name, the release date of the MP, MP Version, and the date downloaded and installed in the client's environment. As an Excel file this data can be quickly and easily imported into SQL in a new table and used to generate a report.

After downloading the management packs as an .msi file and double-clicking on the .msi file to launch its extraction you will note two interesting questions as you run through the extraction process. The first is whether you want to make the MP available to Just You or to Everyone, and the second question is where you want to extract it to. The default extraction location is %Program Files%\MOM 2005 Management Packs\<Name of the MP> so don't be confused as many people are after extracting the MP because you look for the extracted files in the %Program Files%\Microsoft Operations Manager 2005\Management Packs directory.

Importing Management Packs

Once you have identified the management packs that you wish to work with, the next step is to import them into your MOM management group using the Administrator console or the ManagementModuleUtil.exe found in the %Program Files%\Microsoft Operations Manager 2005 directory on your MOM management

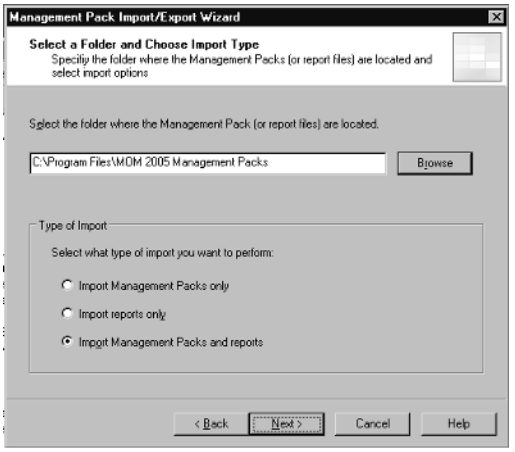
server. If you have already installed MOM Reporting, both management pack .akm file and their corresponding reporting .xml file can be imported in the same process. If MOM 2005 Reporting isn't installed, you will have only the option to import the management pack.

NOTE

There is currently no way within MOM 2005 to officially uninstall a management pack and all the data associated with it, so always plan your MP deployments and install the MP first in a lab environment to allow you to get to know the rules included in it. With any kind of operations management software, you will never be able to confirm with 100% certainty in a lab environment what the outcome will be when you install the same software in your production environment since very few organizations have a lab that is a complete replica of production. That said, take advantage of virtualization software like Microsoft Virtual Server 2005 or VMware ESX or GSX, because these applications will allow you to build and host a multiserver lab environment on a single physical server in very little time. Want to know more about virtualization? Check out *Virtualization with VMware™ ESX Server™* (Syngress Publishing, ISBN: 1-59749-019-9).

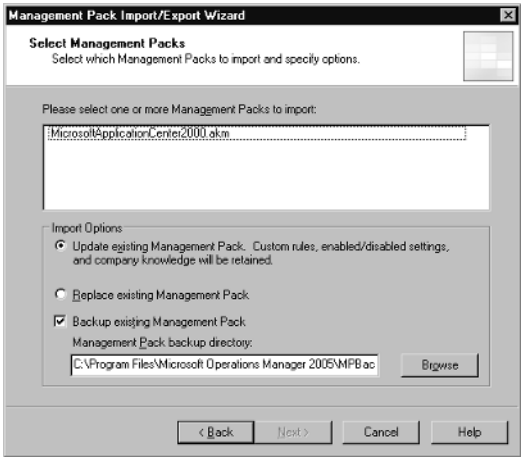
Once your testing and evaluation of a management pack is complete, the actual import process is quite simple as you can see from the following steps. Within the Administrator console, right-click on the Management Packs node and select **Import/Export Management Pack**. Select to import management packs (or reports) (note that the option to export is also available) and then either type the path to where the Management Pack Files are located or browse to it. Then in the Types or Import section shown in Figure 5.24, select the action you would like to perform. In this example, all options are available to you because MOM Reporting is installed in this environment. For the purposes of this example, we will select to import both the management pack and the reports.

Figure 5.24 Importing Management Packs



Next in the Select Management Packs dialog box, you will be prompted to select the .akm file that you want to import and to define your import options as shown in Figure 5.25. If this is the first time that you are importing the MP, then these options don't mean a great deal and you can deselect the Backup option and leave the default import option selected. However, if you have downloaded an updated MP that was released to the Web and you already have an older version of this same MP installed, these options become very important.

Figure 5.25 Setting MP Import Options



Updating Management Packs

When updating an existing MP, you always want to ensure that you have a backup of the currently installed MP simply for recovery, so ensuring that the Backup option is selected is a must. Next you must select an Import option based on your knowledge of changes to the existing MP. If you have followed the best practices that have been discussed in this chapter, then you will never have made changes to any built-in rules, but instead will have copied those rules and will have modified the copied version after disabling the original rule. If you have followed this best practice then you will want to select the Update Existing Management Pack option. Now on the flip side, if you haven't followed best practices and you have made changes to the built-in rules and you have made a mess of the original MP and you simply want to overwrite everything that you have done and get back to a known good state, then you could select the Replace Existing Management Pack option and overwrite everything in the currently installed MP.

In this example, we selected to import only a single management pack, but you do have the ability to import multiple MPs at the same time. Be cautious when importing multiple MPs at the same time, as this could significantly increase the amount of information both collected on monitored systems and also sent back to the management server. Remember that one of the first things that you want to do after importing a new MP is to monitor the volume of information being received by your OnePoint database and identify the rules within the MP generating the most noise as this could be a result of problems within your environment, a misconfigured rule or threshold, or a known issue within your environment and justification to disable that rule or define an override.

Once the MP has been imported you are able to make additional changes to the rules included within it through the Administrator console.

NOTE

It's not uncommon to find that customers want to view reports immediately after you have installed a new MP. Remember that although the reports have been imported and stored in the configuration tables in the OnePoint database, they will not be available until the Data Warehouse DTS job has run and the rules defined to collect information to report on have enough data to allow you to define a report. It's very common for a customer to ask for the creation of some custom reports as part of the consulting engagement or MOM 2005 deployment, but one expectation I always try to set is that this type of deliverable is always a phase-two deliverable, with the first phase focused on the installation and configu-

ration of the MOM management group and the tuning of the installed management packs.

Compatibility with MOM 2000 Management Packs

Although MOM 2005 supports upgrading from MOM 2000 Service Pack 1 (SP1), this is not an option that I would recommend to customers as I have found this to be riddled with issues. As opposed to an upgrade, I would always recommend that clients perform a parallel installation, multihome their agents, and then begin the process of removing the MOM 2000 agents as opposed to upgrading. That said, if for whatever reason you do elect to upgrade your existing MOM 2000 SP1 configuration group to MOM 2005, you should find that your installed management packs upgrade seamlessly and work within your MOM 2005 management group. What will not upgrade to MOM 2005 is your MOM 2000 SP1 Microsoft Access-based reports since there is no upgrade path for this component.

Your existing MOM 2000 SP1 management packs will work in MOM 2005 likely without any modifications; however, bare in mind that these existing management packs will not include any of the new monitoring functionality available in MOM 2005 MPs such as service discovery, state monitoring, and topological diagrams.

The new functionality and features included in MOM 2005 might be reason enough for you to reevaluate your management pack's design priorities and update or rewrite the MP to include support for this new feature set. Some of the new functionality, such as agentless monitoring, should not require any significant changes to your existing rules; however, should you not want to support agentless monitoring, modifications can be made to prevent agentless monitoring from being used within your management pack. Another potential issue that you might encounter in any rules written to leverage scripts are deprecated helper objects. In MOM 2005, a small number of script helper objects have been removed, which may result in scripts failures and the need to rewrite portions of your scripts or the entire script. Part of your migration review should include a review of the supported script helper objects.

Service discovery is one of the new features that you may decide to take advantage of in MOM 2005 to allow you to collect information about your application and its relationships. This information in turn can be viewed in the State Monitoring view within the Operator console and leveraged in MOM 2005 reports that utilize SQL Reporting Services.

State monitoring is another new feature in MOM 2005 that can provide you with real-time health views of your application roles and components. The

Management Pack Wizard, a utility in the MOM 2005 Resource Kit, can be used to help you write and develop management packs to leverage this new state monitoring functionality.

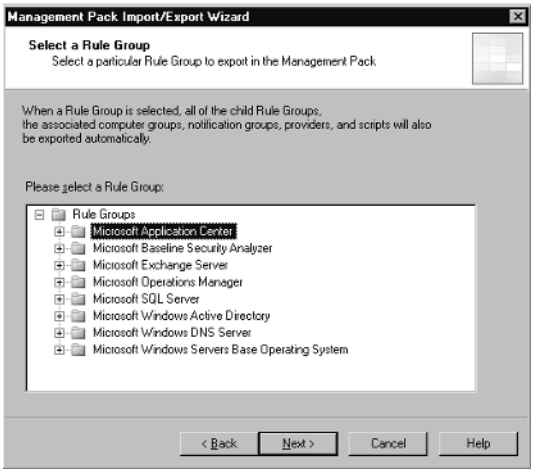
Topological diagrams, usually a big hit with most customers and great for documentation purposes, allow you to create a visual representation of your application's relationships and health and can be viewed with the Operator console and subsequently exported to Microsoft Visio.

Exporting Management Packs

The regular exporting of MPs is no replacement for a regularly scheduled backup on the MOM database and MOM management servers, however it is one way of managing source control over changes made to management packs. The exporting of MPs, however, does provide you with a great deal of flexibility and greatly reduces administrative effort when making changes to rules within your lab environment that you would also like to use, after testing is complete, within your production environment. The ability to export these rules from your lab and then import them into production can save you a significant amount of time as opposed to having to recreate each of the rules.

The process of exporting MPs is quite simple and like importing begins with right-clicking the **Management Packs** node in the Administrator console and selecting **Import/Export Management Pack**. The same process can be followed here as was detailed earlier in the Export MPs section with the exception of choosing Export as opposed to Import. Again, similar to the import of MPs, you will be asked to select the rule group that you want to export but unlike importing, you are able to select only a single MP at a time when exporting as you can see in Figure 5.26.

Figure 5.26 Exporting a Rule Group



Using the Management Pack Notifier

One unique management pack available from Microsoft is the Microsoft Operations Manager MP Notifier, which when installed will alert you to newer versions of installed management packs. A small management pack with only three rules, two event rules, and a single alert rule, this management pack includes a script that runs daily and checks for the versions of the installed MPs. One configuration step is required for this management pack to work, and that is adding one of the MOM management servers to the Microsoft Operations Manager MPNotifier MOM Server computer group.

Summary

Within this chapter you have learned about the underlying components that make up a management pack and how to work with each of these. You should now have a clear understanding of how rule groups correlate to computer groups, and what determines membership in a computer group. This knowledge will assist you when creating your own custom management packs. You have learned about the different event, alert, and performance rules, how to create them, and how to modify them according to best practices. We have also looked at other ancillary management pack components such as views, tasks, and providers, and learned how each of these can be used. With respect to maintenance and ongoing administration you have learned how to import and export management packs and how to determine what rules and rule groups are being received by a monitored agent. This chapter is intended to provide you a baseline of knowledge about management packs so that you can build on this in future chapters when exploring specific management packs such as Exchange, Active Directory, SQL, and OEM-specific MP in later chapters.

Solutions Fast Track

Defining a Management Pack

- ☑ A management pack is a collection of rules and possibly accompanying reports that provide a set of criteria used by MOM agents to help determine what information to collect, act on, and forward to the MOM management server.
- ☑ Rules are categorized into three types within a management pack: event, alert, and performance rules.
- ☑ Some of the key elements of a management pack include events, alerts, and performance rules; product knowledge, state monitoring, views, tasks, and reports.
- ☑ One of the internal mandates at Microsoft is to release a management pack for each application and operating system that they release, and to have the release of the MP happen around the same time the application goes release to manufacturing (RTM).
- ☑ Microsoft has numerous management packs available for the monitoring of their own operating systems and applications and lists these and third-party

management packs on the Microsoft Web site in the Management Pack Catalog.

- ☑ Third-party management packs allow you to monitor non-Microsoft operating systems, applications, and devices such as Linux, UNIX, AIX, Oracle, Antivirus, Cisco, EMC, and Nortel.
- ☑ Agentless management is a new feature of MOM 2005 that allows systems or devices that do not have an agent installed to be monitored. Certain functionality is not supported in agentless managed configurations: monitoring agentlessly through a firewall; descriptions of event log entries on the agentless machine are not displayed; script and command line responses used in timed events must leverage the $TargetComputer$ property.
- ☑ Some management packs such as Active Directory and IIS do not support agentless management.

Working with Management Packs

- ☑ Management packs also often include other components in addition to rules such as tasks, and views that are specific to the management pack.
- ☑ Management packs can be imported and exported from MOM 2005 and are saved as .akm files, and the accompanying reports file is saved as .xml.
- ☑ Console tasks, as the name implies, run in the Operator console and execute on the same computer on which the Operator console is installed.
- ☑ Runtime tasks can be executed either on a management server or on an agent-managed computer. You have more options available to you with runtime tasks than you do with console tasks in that you can select from multiple task types including Command line, Script, Managed Code, and File Transfer tasks.
- ☑ Providers determine how and where to get the data that rules depend on, and MOM exposes the following provider types: NT Event Log, NT Performance Counter, Application Log, WMI Event, WMI Numeric Events, Timed Event.
- ☑ The Microsoft Operations Manager MP Notifier is a management pack designed to alert you to newer versions of installed management packs when they become available.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: I want to have a notification sent to an e-mail address when any alert within a specific rule group has a severity level or error or higher. What's the best way to accomplish this?

A: You have two options for configuring responses. You could modify the properties of each individual event that is configured to generate an alert where the severity level is error or higher, but this would take a considerable amount of time depending on the number of rules. The recommended approach would be to create a single alert rule that looks for a severity of error or higher and fires an alert based on a specified set of criteria.

Q: I have copied a rule included in a management pack but when I paste the rule, the knowledge information is not there. Is this normal?

A: Yes, this is normal. When you copy a rule, the knowledge information does not get copied; however, you have the ability to redefine this knowledge information by right-clicking the Rule Groups folder and selecting Enable Author Mode. In Author mode, when you open the properties of a rule, you will see an additional tab, the Knowledge Authoring tab, that allows you to define the information displayed on the Knowledge tab.

Q: I would like to be able to quickly view all the monitored systems in my environment that meet specific criteria. What is the best way to do this?

A: To view monitored systems based on specific criteria, you can create a view in the Operator console.

Q: I would like to create a series of views in the Operator console for the Active Directory monitoring and administration group within my organization and want them to use these and only these views on an ongoing basis. Is this possible?

A: Yes, this is definitely possible. This can be accomplished by creating the series of views in the Operator console and then saving the console as an .omc file and distributing this console settings file to your Active Directory monitoring and administration group.

Q: I am trying to create a new custom task but can't seem to find the option to do this in the Operator console.

A: New custom tasks can be defined but these are created in the Administrator console, not the Operator console. Once created, you can refresh the Operator console and you should see the newly created task.

Q: I have created a new rule group and created rules within it but the rules don't appear to be received by the monitoring agents. How can I determine what rules a monitored agent is receiving?

A: In the MOM 2005 Resource Kit, there is a utility called the Resultant Set of Rules (rsor.exe), which can be run to determine what rules are being received by a monitored agent. This utility generates a log file that details all the rules being received.

Q: After creating a number of new rules, and running rsor.exe to determine if they are being received, I have noticed that they aren't being received as I would have expected. What might be causing this?

A: After creating new rules, it's important that you right-click the Management Pack nodes and select Commit Configuration changes. This communicates the new rules into the database and allows them to be distributed to your monitored agents. You might also want to look at the application event log on the monitored agent for event id 21240 from source Microsoft Operations Manager to see if new rules have been received recently. You might also want to look at the rule group and see what computer groups it's bound to.

Q: We have spent a significant amount of time creating and testing a custom rule group in our lab environment and are ready to move this over to our production environment. What is the easiest way to do this?

A: Exporting the management pack from your lab environment will allow you to create an .akm file that can then be imported into your production environment. Use the Administrator console to export and import management packs.

Chapter 6

Managing Microsoft Exchange

Solutions in this chapter:

- **Managing Exchange 2000 and 2003**
- **Monitoring Exchange 2000 and 2003**
- **Managing and Monitoring Exchange 5.5**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

The Exchange Management Pack is a series of components that can be imported into Microsoft Operations Manager (MOM). When you import this pack, groups of rules, performance counters, interfaces, reports, and other features are added to MOM, thereby allowing you to monitor and manage elements of the Exchange server and the services and resources it provides.

Some preparation is required to deploy the Exchange Management Pack, but as we'll see in this chapter, its import and configuration are relatively easy. A Configuration Wizard is also available to install, providing a tool that allows you to quickly change settings and determine what to monitor. Once your installation of the Exchange Management Pack is completed, interfaces and rules can be used to monitor events, monitor the health of the Exchange server, and manage availability.

We will also briefly discuss issues regarding Exchange 5.5 and the Exchange 5.5 Management Pack that was made available for MOM 2000. Although the Exchange Management Pack for MOM 2005 does provide methods of communicating with these older servers, this version of Exchange is no longer supported.

Managing Exchange 2000 and Exchange 2003

MOM with the Exchange Management Pack is a very interesting product, especially for relatively large organizations. With MOM and the Exchange Management Pack, you can be proactive by monitoring the performance, availability, and security features of Exchange. The Exchange Management Pack alerts you to events that have a direct impact on server availability while filtering out events that require no action. By detecting, alerting on, and automatically responding to critical events, the management pack helps identify, correct, and prevent possible Exchange service outages.

This management pack was designed to detect indications of a potential service interruption and to immediately send an alert to your Exchange administrator if a service interruption occurs. It can proactively monitor more than 1,600 events, performance counters, services, and Internet protocols, such as:

- Directory Service Access (DSAccess)
- Microsoft Exchange Information Store service
- Extensible Storage Engine (ESE)
- Message Transfer Agent (MTA)
- Simple Mail Transfer Protocol (SMTP)
- Post Office Protocol (POP3)

- Internet Message Access Protocol (IMAP4)

By being able to identify potential problems early, you are better able to deal with them before significant issues result in major downtime and loss of service. The Exchange Management Pack allows you to isolate areas of an Exchange server that may need attention. As we'll see later in this chapter, it also allows you to generate reports that can be useful in determining the current condition and planning the future of your Exchange network.

A nice thing about MOM is that third-party vendors can develop their own packages that can integrate directly into MOM. We suggest you read more about this trend at the Microsoft Operations Manager site at www.microsoft.com/mom.

Overview of the Exchange 2000/2003 Management Pack

Because the ability to share information through e-mail can be vital to the way a company conducts business, people have come to rely on sending messages as a requirement of their jobs and as part of their daily routines. The need for this technology makes the availability and performance of Exchange servers in an organization as much a priority as being able to access files or other network resources. To meet this need, the Exchange Management Pack provides the tools to monitor the health, operation, and usage of servers, databases, and mailboxes.

Using the Exchange Management Pack, you can carry out numerous tasks that allow you to address potential issues, including:

- **Create a performance baseline** This task identifies how Exchange runs normally under proper conditions. By seeing the normal operation characteristics of the server, you can identify potential problems when the Exchange server is operating outside of these known parameters. By having this information early, you can take preventive measures before a problem actually exists.
- **Acquire performance metrics** These metrics monitor the current performance of Exchange servers and related services to ensure that Exchange and the network are functioning normally or indicate that they are in need of upgrades.
- **Evaluate peak hours of operation** This task shows when Exchange is being used most often and when the workload of the server is at its highest.
- **Manage configuration** This task ensures that all Exchange servers on a network are configured to function and work together properly. Managing configuration ensures that each server is exchanging mail between servers, that each mailbox is available, and that each server is performing other functions normally.

Exchange Management Pack Components

To provide the various features of monitoring and managing Exchange servers, resources and services, the Exchange Management Pack includes a number of different components. These components include graphical user interfaces, rules, reports that can be generated, and other features that are provided when the pack is imported into MOM.

The Administrator Console, an interface that is used to configure MOM 2005 and the Exchange Management Pack, allows you to view information about Exchange on the network. Using this tool, you can view which Exchange servers are on your network, deploy agents, manage user privileges, and (as we'll see later in this chapter) create, import and export management packs.

Interfaces

The Operator Console is another interface that is used to monitor the health of systems, identify potential problems, and provide recommended resolutions to various issues. When an alert is displayed in the Operator Console, the **Product Knowledge Base** tab can be clicked to access information on how to solve the problem. The Knowledge Base available through the Exchange Management Pack provides technical information on solving known issues that may result on an Exchange server. The information available through this component can aid in troubleshooting issues. Although Microsoft initially provides all of the information in the Knowledge Base, you can add information that is specific to your company.

In addition to these consoles, there are also Web-based interfaces that are accessible using a Web browser. The Web Console can be used to view a subset of the features available through the Operator Console, allowing you to view and modify alert statuses, view the Knowledge Base, and monitor the status of a computer. The Reporting Console enables you to view alerts, events, and reports. As events change, you can also use this Web-based console to subscribe to various reports and receive updated information. Because these two consoles are accessed through a Web browser, you can access their functionality from anywhere on the network.

Rules and Rule Groups

Most of the information accessed through the various consoles is stored in the MOM database. As changes are made using the Administrator Console, modifications to the Knowledge Base and rules on monitoring and how MOM reacts to various events are imported into the database. The rules are then pushed to each of the Exchange servers running MOM agents.

The rules specified through the Administrator Console determine how MOM will collect and handle various forms of data and events. When the MOM server receives this information, it will use the rule to determine how it will respond to it, such as sending an

alert or writing information to an event log. Several different types of rules may be stored in the MOM database, including:

- **Event Rules** These rules are used to generate an alert or respond to specific events when they occur.
- **Alert Rules** These rules are used to respond to specific alerts when a specific value is reached.
- **Performance Rules** These rules are used to collect data on an Exchange server's performance. When a specific value is reached (such as disk space usage) or exceeded, MOM will respond to it by sending an alert.

The rules created and modified using the Administrator Console are organized into groups. These Rule Groups include:

- **Availability Monitoring** This group consists of rules on testing the availability of Exchange services, front-end servers, MAPI logon, connections to the database, mailbox availability, and mail flow.
- **Exchange Event Monitoring** This group consists of rules dealing with events in Exchange, which are written to an event log.
- **Health Monitoring and Performance Thresholds** This group consists of rules dealing with server health and configuration, security settings, disk space, and mail queue thresholds. By setting these rules, you can identify problems with various components of an Exchange server by setting alerts that notify you when a threshold has been exceeded.
- **Performance Counter Logging Rules** This group consists of those rules that monitor the usage and performance of an Exchange server. This includes rules dealing with monitoring clients, server resources, antivirus, and usage of the public folder store.
- **Report Collection Rules** This group contains rules on information compiles for various reports on database size, configuration, mailbox statistics, message tracking, and other data.

Deploying the Exchange Management Pack

The first step in deploying any new software on a network or computer system is preparation. As with any installation of a new product, you should first document any existing configurations, especially if you're upgrading from a previous version. It is also wise to back up any servers on which the product is being installed. These measures will aid you in restoring the system to a previous state, if a problem should occur during the installation.

Another part of your deployment preparation involves making decisions on the requirements of your organization. Different companies will have different objectives and performance expectations that will help you in configuring the Exchange Management Pack for acquiring data, determining what will be monitored, and determining which reports will need to be generated.

Because alerts can be sent when a particular event occurs, you will need to decide who will receive them and what kind of notification will be given. In administrating alerts, Microsoft recommends that you follow these steps:

1. Identify the administrators in your organization who need to be notified when there is a problem with Exchange
2. Add each of these administrators to the MOM Operators security group
3. Configure each of the administrators with a paging and messaging schedule
4. Add each of them to the Mail Administrators notification group

Once these steps are completed, you should then plan how the Exchange Management Pack will be deployed. In creating this plan, you will need to decide the following:

- Decide which servers will be monitored
- Decide which servers that will be used for monitoring Exchange
- Determine which members of the IT staff will be responsible for installing the Exchange Management Pack
- Ensure that the installation team has the proper permissions to perform the installation
- Make a schedule of when different servers will have the Exchange Management Pack installed
- Find any issues that are specific to your organization that may impact the effectiveness or success of installation and configuration

Once you've made the necessary decisions and ensured that your system can be restored in the event of a problem during installation, you should be ready to import and configure the Exchange Management Pack.

Importing the Exchange Management Pack

Before you can begin configuring and using the features available through the Exchange Management Pack, it must be imported into the Microsoft Operations Manager. Once imported, you will then be able to set what will be monitored on your Exchange server, inclusive to what services are to be monitored, as well as perform tests on mailbox availability and mail flow.

To import the management pack, you first need to acquire a file called Exchange Management Pack.akm. This file can be found on the MOM installation CD, or you can download it from Microsoft's Web site. The file needs to be copied to the Microsoft Operations Manager consolidator server, where you will then begin the process of importing it.

From the Start menu, you select **Programs | Microsoft Operations Manager 2005** and then click the **Administrative Console** menu item. When the Administrative Console opens, you expand the **Microsoft Operations Manager** in the console root. By expanding this entry, you will see an item named **Management Packs**, which you would then right-click on to display a context menu. On this menu, you click **Import/Export Management Pack** to start a wizard that will take you step-by-step through the process of importing the Exchange Management Pack.

When the **Management Pack Import/Export Wizard** opens, you will first see a welcome screen. Clicking the **Next** button will display the Import or Export Management Packs screen, which should have an item called Import Management Packs and / or reports selected. Once you've verified that this is selected, you would then click **Next** to continue.

The next screen is the Select a Folder and Choose Import Type dialog box. By clicking the **Browse** button, you can browse the hard drive(s) to specify the folder where you copied the *Exchange Management Pack.akm* file. Once you've located the folder, selecting **Import Management Packs only** from the Type of Import on this screen will specify that you will be importing management packs from the folder.

Clicking the **Next** button will display the Select Management Packs screen. On this screen you should see a selection named Exchange Management Pack.akm, indicating that the correct folder was selected earlier and the import file was found. After you click **Next** and then click **Finish**, the installation of the file will proceed. When the installation is completed, a Description pane will appear to show that the installation of the management pack was successful. When you click **Close**, the import process of the pack is completed, and you're ready to begin configuration.

Running the Configuration Wizard

The Configuration Wizard provides a graphical interface that takes you step-by-step through the process of configuring the Exchange Management Pack. Using this tool, the rules and scripts that are used to monitor Exchange services are configured, inclusive to those dealing with message tracking, mail flow options, and the availability of mailboxes and front-end servers. A network administrator with little to no experience can use this tool to set up the Exchange Management Pack quickly and easily.

Installing the Configuration Wizard

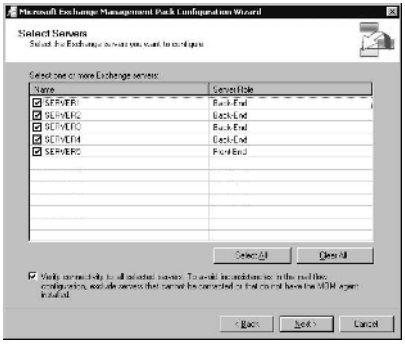
The Configuration Wizard is included in the Tools folder of the Microsoft Operations Management CD. It can also be downloaded from Microsoft's Download Center at www.microsoft.com/downloads. To install the wizard, you would copy the Configapp.msi file to any computer that has Exchange System Manager and .NET Framework 1.1 installed. Before running this file on the machine you've copied it to, you need to ensure that the following prerequisites are also met on each machine the wizard will run on:

- The user account being used has Exchange full administrator rights at the organization or administrative group being configured.
- The user account has local administrative rights to each of the Exchange servers being configured so that the Configuration Wizard can write to the Registry.
- Each Exchange server has the Remote Registry Service running. Once these prerequisites are met, you would then double-click the **Configapp.msi file** that you copied to each machine, which then installs the Configuration Wizard.

Running the Configuration Wizard

Once the Configuration Wizard has been installed, it can be accessed through the Start menu of the Exchange server. After you select **Programs | Exchange Management Pack** and then click **Exchange Management Pack Configuration Wizard**, the program will start, and a welcome screen will be displayed. After clicking the **Next** button, you can select whether you'd like to work with servers in all administrative groups or select a particular administrative group to work in. Once you've made your selection and clicked **Next**, you are presented with a listing of servers that can be configured, similar to that shown in Figure 6.1.

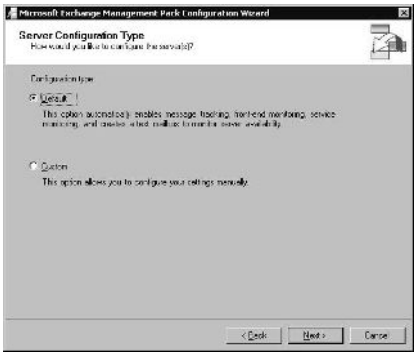
Figure 6.1 The Select Servers Screen of the Configuration Wizard



As the screen in Figure 6.1 indicates, the Exchange servers on your network appear in a listing, with a separate column indicating the server's role. A checkbox appears beside each entry, which can be clicked, allowing you to check which ones are to be configured by the wizard. Any servers that you don't want configured or may be unavailable can then be unchecked and excluded from configuration. Another checkbox at the bottom of this screen allows you to decide whether connectivity to the servers you've selected should be verified. It is checked by default.

Clicking the **Next** button will display the Server Configuration Type screen, which allows you to select whether you want to use default configuration options or customize your settings manually (see Figure 6.2). If the Default option is selected, a test mailbox is created to test the availability of servers, and message tracking and service monitoring are enabled. However, with this option, only a single mailbox is monitored for availability on each server. If you want to monitor more than this, you should choose **Custom**, which will allow you to monitor mailboxes on a per-server or per-store basis. The Custom option will also allow you to control which services are monitored on servers, as we'll see later.

Figure 6.2 The Server Configuration Type Screen of the Configuration Wizard

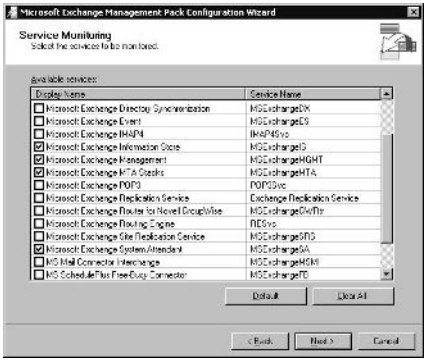


Clicking **Next** provides you with a screen that allows you to decide which features (or properties) will be configured. A checkbox appears beside each item on the Properties screen, which when checked controls which screens will appear to you later in the wizard. The items available to choose from on this screen are:

- Message tracking
- Front-end monitoring, which is enabled only if one or more of the selected servers is a front-end server
- Service monitoring
- Mailbox availability
- Mail flow

The options you choose to configure on this screen will control what screens appear afterward in the wizard. If **Message tracking** and/or **Front-end monitoring** are checked, then clicking **Next** will allow you to select which servers will have these features enabled or disabled. If these features aren't chosen to be configured, clicking **Next** will bring you to the Service monitoring screen, which is shown in Figure 6.3.

Figure 6.3 The Service Monitoring Screen of the Configuration Wizard

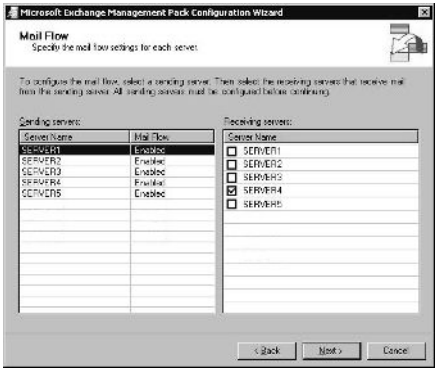


The Service Monitoring screen provides a listing of all of the services that can be monitoring with the Exchange Management Pack, with several services. The Configuration Wizard has six services that are selected by default, and it can be reset to these selections by clicking the **Default** button on this screen. The services monitored by default are Microsoft Exchange Information Store, Microsoft Exchange Management, Microsoft Exchange MTA Stacks, Microsoft Exchange System Attendant, Simple Mail Transfer Protocol (SMTP), and World Wide Web Publishing Service.

When the Custom configuration option is used and the Mailbox availability option has been selected, clicking the **Next** button will display a screen that allows you to configure how the availability of mailboxes is monitored. Using this screen you can choose whether mailbox availability is monitored on a per-server or per-store basis, or if no store monitoring is used. If you want all mailbox stores to be monitored on the Exchange server, you would select the per-store option. Using the per-server monitoring will have the Exchange Management Pack monitor the availability of a test mailbox that's created.

Upon clicking **Next**, the final configuration screen that you'll encounter using the default properties selected earlier is the **Mail Flow** dialog box. This screen will appear regardless of whether you selected the Default or Custom configuration option earlier in the wizard. As Figure 6.4 indicates, the left side of this screen is used to select the server that will send mail, and the right side of the screen is used to select which servers will receive mail from that particular sending server. By specifying the flow of mail that will occur between these servers, the Exchange Management Pack can then perform mail flow tests between those servers.

Figure 6.4 The Mail Flow Screen of the Configuration Wizard



Once you've specified the mail flow settings of each Exchange server on your network, you can then click the **Next** button to view a summary of all the settings made in the Configuration Wizard. This allows you to review the settings before they are set, and if necessary, click the **Back** button to toggle through the screens and modify any settings you've made. If everything is configured as you wanted, you can then continue by clicking **Next** to finish the configuration process using the wizard.

Best Practices According to Microsoft

- Generally, you will not need to make significant changes to the rules and scripts in the Exchange Management Pack, but if you do need to make such modifications, it is best to copy each rule being changed and modify them outside of the rule group, and then disable the original rule. If a problem occurs in the modified rule, you can then delete the new rule and enable the original rule. Because reimporting the Exchange Management Pack will overwrite any changes, you should also document which of the original rules were disabled so that you can disable them again after the reimport.
- Ensure that the Mailbox Access Account has proper permissions to read and write to the directory where temporary MAPI logon profiles are created. This directory is %systemroot\temp\exmppd. You should verify that your account has the proper permissions by logging on to the server using the Mailbox Access Account and create a test file in this directory.
- Ensure that the Mailbox Access Account has local logon rights on each Exchange Server, as this is required for the MAPI logon and Mail Flow tests.
- Do not configure Send As and Receive As permissions on the Organization object to Deny as the Mailbox Access Account won't be able to log on to the Exchange server. In such a case, the MAPI Logon verification tests will fail.
- MAPI logon tests require a monitoring server is able to access a domain controller. If a monitoring server is unable to access a domain controller or doesn't receive a timely response from it, then the MAPI logon test will fail.

- Synchronize system clocks to avoid issues related to timing. If the time isn't synchronized between servers, the Mail Flow tests may report latency issues. Servers can be synchronized using the Net Time command, using the following syntax:
  `net time \\server fully qualified domain name /set /y`

Monitoring Exchange 2000 and 2003

The scripts, rules, and other features installed through the Exchange Management Pack enable you to monitor a significant number of elements related to an Exchange environment. As we discussed earlier, monitoring Exchange can be done manually by viewing information provided through interfaces or automatically by having notifications sent when a particular event or alert occurs. In looking at these occurrences that may indicate problems with Exchange servers or services, you will find that they can be broken down into several categories:

- **Monitoring events** Filtering and viewing tools are used to monitor the various events occurring in the Exchange environment.
- **Monitoring the health of an Exchange server** The health and performance of the server are measured and tracked using rules and metrics. The information acquired from monitoring this data can be used for identifying potential points of failure and areas where changes need to be made to accommodate growth.
- **Managing Exchange Availability** Rules and scripts are used to monitor the availability of services, mail flow, database operations, and the functionality of Exchange servers.

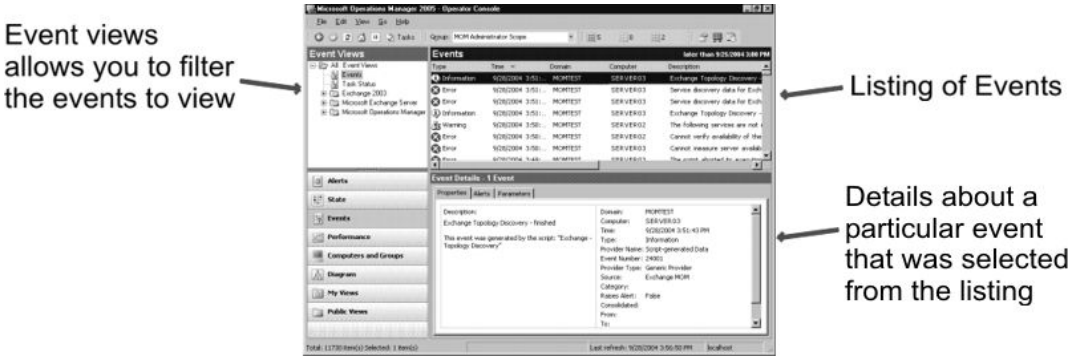
Monitoring Events

Earlier in this chapter, we discussed how the Operator Console allows you to monitor the health of systems and identify potential problems. By clicking the **Events** button on this console, you can view information on various events logged by Exchange servers that are being monitored. As Figure 6.5 shows, the **Event Views** pane of the Operator Console allows you to select the events that will be displayed in the listing to its right. By clicking different categories of events in the Event Views pane, the related information on those events is displayed in a listing to the right of this pane. Selecting a particular event from this list will display details in the pane shown in Figure 6.5, which is in the bottom right of the console.

The Event Views pane of the Operator Console provides two different views of monitoring events that have occurred on Exchange servers that are being monitored:

- **Events** This view provides a listing of information, warnings and errors that are collected from Exchange servers being monitored.
- **Task Status** This view provides information, warnings, and errors on events related to tasks that are scheduled by Microsoft Operations Manager.

Figure 6.5 The Operator Console Can Be Used to View Events



Monitoring the Health of an Exchange Server

By clicking the **Performance** button of the Operator Console, you can also view information on various performance-related data acquired from Exchange servers that are being monitored. This information is acquired from rules, which is another component that's installed with the Exchange Management Pack. As we discussed earlier in this chapter, rules can be used to monitor performance indicators, which are values representing aspects of the Exchange server, and can be enabled or disabled as needed. The groups of rules dealing with the health of an Exchange server include:

- **Free Disk Space Thresholds** These rules allow you to view information on the disk space of the Exchange server.
- **Mail Queue Thresholds** These rules contain information on mail queues in Exchange, inclusive to the size of the queue and any latencies that exist.
- **Server Configuration and Security** These rules allow you to view information on security settings and the configuration of the Exchange server.
- **Server Performance Thresholds** These rules contain information on the overall performance of the Exchange server.
- **SMTP Remote Queue Thresholds** These rules allow you to monitor outbound queues as well as their growth and sizes.

- **Windows Updates** These rules allow you to verify that all of the monitored Exchange servers have the same updates installed to them

Free Disk Space Thresholds

The amount of disk space on a server is always an important issue on a network. Alerts in this group provide information on the usage of disk space and inform you of when the amount of free space has dropped below a specific value. Because a lack of disk space can affect the performance and functionality of a server, there are a large number of rules associated with this particular group, including:

- **Check free disk space**, which is a script that runs every 30 minutes by default to check the percentage of disk space on an Exchange server's local disks.
- **Exchangespace**, which generates an alert when the percentage and amount of free disk space for the volume containing transaction log files and queues are below a specific value. A 9978 MOM event is generated when this occurs, and an alert is created.
- **Exchange03 Simple Mail Transfer Protocol (SMTP) Queue and Transaction log drive is very low on disk space**, which generates an alert when the percentage and amount of free disk space for the volume containing transaction log files and queues are critically below a specific value. A 9977 MOM event is generated when this occurs, and an alert is created.
- **Exchange 2003 Transaction log drive is low on disk space**, which generates an alert when the percentage and amount of free disk space for the volume containing transaction log files are below a specific value. A 9976 MOM event is generated when this occurs, and an alert is created.
- **Exchange 2003 Transaction log drive is very low on disk space**, which generates an alert when the percentage and amount of free disk space for the volume containing transaction log files are below a specific value. A 9975 MOM event is generated when this occurs, and an alert is created.
- **Exchange 2003 Simple Mail Transfer Protocol (SMTP) Queue drive is low on disk space**, which generates an alert when the percentage and amount of free disk space for the volume containing SMTP queues are below a specific value. A 9974 MOM event is generated when this occurs, and an alert is created.
- **Exchange 2003 Simple Mail Transfer Protocol (SMTP) Queue drive is very low on disk space**, which is used to indicate a more urgent situation than the previous rule, as free disk space has become critically low. An alert is generated when the percentage and amount of free disk space for the volume containing SMTP is below a specific value. A 9973 MOM event is generated when this occurs, and an alert is created.

- **Low free disk space**, which generates an alert when the percentage and amount of free disk space for any volumes that do *not* contain transaction log files or queues are below a specific value. A 9972 MOM event is generated when this occurs, and an alert is created.
- **Very low free disk space**, which is used to indicate a more urgent situation than the previous rule, as free disk space has become critically low on volumes that don't contain transaction logs or queue files. A 9971 MOM event is generated when this occurs, and an alert is created.

Mail Queue Thresholds

The rules making up this group are used to test mail flow and generate errors when there is a disruption in the flow of mail between two or more servers, or when a particular alert has a minimum severity level of Error. The various rules in this group include:

- **Exchange Information Store service Queue of Messages to MTA > 50**, which uses the MSExchangeIS Transport Driver performance object to track the number of message that are in transit.
- **Exchange 2003: SMTP: Local Queue > 50**, which uses the SMTP Server object and Local Queue Length counter to track messages that are waiting to be delivered to the Microsoft Exchange Information Store service.
- **Exchange 2003: SMTP: Local Retry Queue > 50**, which tracks the SMTP Server object and its Total Retry Queue Length counter to monitor the queue of messages that are waiting and have previously failed to be delivered.
- **Exchange 2003: SMTP: Messages Pending Routing > 50**, which uses the SMTP Server object and its Messages Pending Routing counter to track messages that have been categorized by not routed.
- **Exchange 2003: SMTP: Messages in SMTP Queue Directory > 500**, which uses the SMTP NTFS Store Driver object and the Messages In Queue Directory counter to track the message number of the queue stored on the physical disk.
- **Exchange 2003: SMTP: Remote Queue > 500**, which uses the SMTP Server object and the Remote Queue Length counter to track remote queues that are used to transfer messages to other servers. The value of this counter is the total for all remote queues.
- **Exchange 2003: SMTP: Remote Retry Queue > 500**, which uses the SMTP Server object and Remote Retry Queue Length counter to track the messages that are in the remote queue and cannot be sent to the destination server.

- **Information Store Queue of Messages from MTA > 25**, which uses the MSExchangeIS Transport Driver object and the Current Message From MSExchangeMTA counter to track messages that are currently in transit from the MTA to the Exchange store.
- **Information Store Transport Temp Table Entries > 600**, which uses the MSExchangeIS Transport Driver object and the TempTable Current counter to track the number of entries in the Microsoft Exchange Information Store service Temp Table.
- **Mailbox Store: Send Queue > 25**, which uses MSExchangeIS Mailbox object and the Send Queue Size counter to track the messages that are waiting to be transferred from the Microsoft Exchange Information Store service to the IIS.
- **Mailbox Store: Receive Queue > 25**, which uses the MSExchangeIS Mailbox object and its Receive Queue Size counter to monitor the number of messages in the mailbox store receive queue.
- **MTA Queue Length per Connection > 50**, which uses the MSExchangeMTA Connections object and the Queue Length counter to track the number of outstanding messages that are queued to be transferred to the database and the Pending Reroute queue.
- **MTA Work Queue > 50, which** uses the MSExchangeMTA object and the Work Queue Length counter to track the messages that are waiting to be processed by the MTA.
- **Public Folder Replication: PF Receive Queue consistently > 10 deep**, which uses the MSExchangeIS Public object and the Receive Queue Size counter to track the Public Folder Replication Receive queue. Generally, this queue should have a value that is near zero, and greater values may indicate that the public folders aren't synchronized between the other Exchange servers on a network.

Server Configuration and Security

The rules in the Server Configuration and Security group are used to test for errors in the configuration and security settings of Exchange servers. The rules are used to run scripts and return results that test various aspects related to these areas. The rules in this group include:

- **Check for existence of mailboxes on Front-End Servers**, which runs a script that searches for mailboxes on front-end servers.
- **Exchange Transaction Log files are equal to or older than the maximum days allowed**, which runs a script that generates an alert if log files are equal to or older than the maximum days configured in the settings.

- **IIS Lockdown was not found on a server**, which indicates that Exchange did not run the IIS Lockdown Tool on a Windows 2000 server. This tool isn't used on newer server, and it applies only to Exchange servers running on Windows 2000 Server.
- **Message Tracking is not enabled**, which indicates that Message Tracking is not enabled, meaning that undelivered messages and troubleshoot mail flow problems cannot be tracked.
- **Message Tracking Logs have "Everyone" group listed in the ACL permission**, which indicates that users in the Everyone group has the ACL (Access Control List) permission to read the Message Tracking Log.
- **SMTP directories are not on an NTFS formatted drive**, which runs a script that checks whether the Queue, Pick Up, and BadMail SMTP directories are on an NTFS file system drive.
- **SSL should be required to secure HTTP access to the Exchange server**, which is used to generate an alert if the server is configured to allow non-SSL data transmission of sensitive data.
- **URLScan ISAPI filter is disabled**, which indicates that the URLScan Internet Server Application Programming Interface (ISAPI) filter is not running. This filter is necessary for only computers running Windows 2000 and is used to prevent security from being compromised on Web servers.
- **Verify that Message Tracking is enabled**, which runs a script that checks whether Message Tracking is enabled.
- **Verify that SMTP Virtual Server cannot anonymously relay (spam prevention)**, which runs a script that determines whether anonymous relay is allowed on each SMTP virtual server.
- **Verify that the IIS lockdown wizard started**, which runs a script that's used to detect whether the IIS Lockdown Tool has been started on a Windows 2000 Exchange server. If this tool has not been started, event 8144 is generated.
- **Verify that the URLScan ISAPI filter is installed and running**, which runs a script that indicates whether the URLScan ISAPI filter is running on an Exchange Server.

Server Performance Thresholds

The Server Performance Thresholds group contains rules that are used to check counters that are used to measure the performance of a server. These counters can indicate whether a problem exists on the server by measuring such things as reads and writes to a disk and CPU usage. By generating an alert when a particular threshold is exceeded, notification

can be sent so that you can deal with a potential problem. The rules included in this group include:

- **Average CPU > 90% for 15 minutes**, which generates an alert if the amount of time the CPU is idle is less than 10%. If the CPU is active more than 90% of the time, it may indicate increased server load or continuous execution of a thread.
- **Disk Read Latencies > 50 ms**, which indicates that latencies greater than 50 milliseconds have been detected.
- **Disk Write Latencies > 50 ms**, which generates an alert when disk write latencies exceed 50 milliseconds.
- **DSAccess:LDAP Search Time > 50 ms avg. over 5 minutes**, which indicates the search time of queries over LDAP that originated from DSAccess is above 50re than five minutes. This shows that queries are experiencing lengthy search times and may indicate a problem if other issues (such as growing SMTP queries) are also detected.
- **Information Store Private Bytes > 1 GB**, which indicates that a process has been allocated a number of bytes that cannot be shared, and this amount has exceeded 1GB.
- **MSExchangeIS:RPC latency > 200 ms**, which checks for latency in RPC requests every minute. An alert is generated if the latency over five minutes exceeds 200 nds.
- **MSExchangeIS: RPC Requests > 25**, which checks the number of RPC requests that are serviced by the Microsoft Exchange Information Store service. Although the service can handle up to 100 RPC requests at a time, the number is normally below 10, so higher numbers may indicate a problem.
- **Outlook Mobile Access: Last response time > 60 sec**, which indicates that an Outlook Mobile Access server's response time is greater than 60 seconds.

SMTP Remote Queue Thresholds

This group of rules works with SMTP remote queues on Exchange servers and uses scripts to check their state and health. If the amount of mail queued to one location exceeds a specific amount, an alert is generated. The rules in this group are:

- **Alert for problems in remote SMTP queues**, which indicates that the number of messages in a queue has exceeded a specific amount (with 200 messages being the default).
- **Verify remote SMTP queues**, which runs a script on an hourly basis to determine the state of the SMTP queue.

Managing Exchange Availability

There are several groups of rules that deal with the availability of systems and services on your Exchange server, which are installed when the Exchange Management Pack is imported into MOM. These groups of rules consist of:

- **Mail Flow**, which uses scripts to send test messages between Exchange servers on the network
- **Exchange Services**, which have rules that check the various services provided by Exchange
- **MAPI**, which contains rules that determine whether MAPI clients can access Exchange databases
- **Database**, which contains rules that check to see whether a database is connected or disconnected
- **Outlook Web Access**, which uses rules and scripts to determine whether Outlook Web Access on Exchange front-end servers is functioning properly
- **Outlook Mobile Access**, which uses scripts to log on as a client to ensure that Outlook Mobile Access is functioning normally
- **Exchange ActiveSync**, which uses scripts to logon to Exchange ActiveSync

Mail Flow

The rules dealing with mail flow utilize a variety of scripts that are used to monitor availability by sending test messages between sending and receiving Exchange servers. By sending messages back and forth between mail servers, you can be determine if mail is being properly sent and received and thus show that the Exchange servers are functioning as they should be.

Exchange Services

As we saw when we discussed the Configuration Wizard, there are a significant number of rules that can be configured to test Exchange services. Once the services to be tested are selected in the wizard, rules are applied to test the availability of these services. At timed intervals, scripts are run to determine if a particular service is running. If a service has stopped, an alert is generated.

MAPI

This group contains rules to determine if a MAPI client can log on to an Exchange database, thereby verifying if the Exchange database and Active Directory is available and can be accessed.

Database

This group consists of two rules that determine whether Exchange databases are connected or not. When a database can't connect or is disconnected, an alert is generated so that notification can be sent.

Best Practices According to Microsoft

- When monitoring Server Availability, you should monitor the server heartbeat, monitor front-end servers, ensure that MAPI logons can be performed, perform mail flow tests, ensure that services aren't terminated unexpectedly, and verify that services are running and databases are mounted.
- When monitoring the services that are running on an Exchange server, you should configure a list of services that are to be monitored on each server, and have an alert generated when a particular service fails to run.
- When monitoring mailboxes, rules can be used to run scripts that log on to mailboxes. Logging in to the mailbox of a test account is important to verify several issues: that the client can connect to the server, that the Exchange server is running, that the database is mounted, and that Active Directory is functioning as expected.
- To monitor the health of a server, rules can be used to run scripts that test free disk space, mail queue and performance thresholds, configuration and security, and SMTP queues.
- When you are monitoring free disk space, tests of free disk space are conducted on several objects: all disks, log disks, and SMTP queue disks. The test monitors counter thresholds that you specify.
- To monitor the configuration and security settings of an Exchange server, you should verify that the IIS Lockdown Tool started, the URLScan ISAPI file is installed and running, message tracking log shares are locked down, and SMTP Virtual Server can't anonymously relay. You will need to determine that mailboxes are on front-end servers and that SMTP directories are on NTFS drives You also will need to determine if SSL is required and make sure that message tracking is enabled.

Generating Reports

MOM includes many Exchange-specific reports to help you quickly identify and correct Exchange issues. With these reports, it's possible to analyze and graph performance data to understand usage trends, perform accurate load balancing, and manage system capacity.

The following reports are available in the Exchange Management Pack:

- **Health monitoring and operations report** Get a summary of Exchanger availability, and configuration of Exchange servers, databases, and mailboxes.
- **Server availability report** Find out the percentage of server availability for computers running Exchange d unavailability is listed along with the reasons that the servers were unavailable.
- **Usage and health report** Get information about server usage and the health of computers running Exchange 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.

Additional Exchange Management Pack reports include mailbox and folder sizes, disk usage, mailboxes per server, and traffic analysis.

The reports provided through the Exchange Management Pack allow you to view a summary of information, which has been acquired over a period of time and stored in the MOM data warehouse database. When a report is created, the information in this database is queried, and a summary of the formatted data is compiled into a report. Although many of the reports that may be commonly used by your organization are included with the Exchange Management Pack, other custom reports can be created or acquired from third-party sources.

Managing and Monitoring Exchange 5.5

On December 31, 2005, Microsoft stopped supporting Exchange 5.5. Because it is a system that's no longer supported, it follows suit that no Exchange 5.5 Management Pack exists for MOM 2005. However, an edition for MOM 2000 can still be found on the Microsoft Web site at www.microsoft.com/downloads. This allows you to use a previous version of MOM on Exchange 5.5 running on Windows 2000 Server or Windows 2003 Server. In this section, we'll discuss the installation of the Exchange 5.5 Management Pack for MOM 2000, as well as components of the Exchange Management Pack for MOM 2005, which provides some support in connecting to Exchange 5.5 servers.

Because Microsoft no longer supports Exchange 5.5, it is best to upgrade from this unsupported version to the latest version of Exchange. If you have reasons for keeping a legacy version of the messaging system on your network, however, all is not lost.

Components do exist in MOM 2005 that allow newer servers with later version of Exchange to communicate with and monitor Exchange 5.5 servers.

Overview of the Exchange 5.5 Management Pack

When the Exchange 5.5 Management Pack is installed on MOM 2000, it enables you to monitor the availability, performance, security, and configuration of Exchange 5.5 servers. Using the components in the pack, you can perform similar functions to those we discussed earlier in this chapter. The Exchange 5.5 Management Pack also allows you to identify potential problems on this legacy system before a major loss of service occurs.

The Management pack also enables you to monitor the server using performance counters that provide values related to various components of the system. Using performance thresholds, you can identify services and areas of the server that may require attention or possible upgrading (such as upgrading the server or simply the hard drive). As we discussed earlier in this chapter, it is wise to create a performance baseline after initially installing the Management Pack to acquire information related to how your server runs normally so that it can then be compared with other performance measurements taken at a later date.

Importing the Exchange 5.5 Management Pack

Although there are some differences, importing the Exchange 5.5 Management Pack into MOM 2000 is similar to the steps we discussed earlier when we covered importing the latest version earlier in this chapter. To import the Exchange 5.5 Management Pack, you will need to be a member of the Administrators local group or a user with sufficient privileges to allow the pack to be installed, which will require writing data to the registry and areas of the hard disk.

Importing the Management Pack begins by opening the Microsoft Operations Manager Administrative Console in Microsoft Management Console. From here, you can then click the **Microsoft Operations Manager (Default)** node to expand it, and then expand the Rules subnode. Once this has been expanded, you right-click on the **Processing Rule Groups** subnode and select **Import Management Pack** from the menu that appears. This will open a dialog box that provides instructions, and where you would locate the file named **Microsoft Exchange.AKM**, which is used for importing the various components of the Exchange 5.5 Management Pack.

Monitoring Exchange 5.5 Components in MOM 2005

The Exchange Management Pack for Microsoft Operations Management 2005 offers some components that are designed for networks that use some Exchange 5.5 servers. The Microsoft Transfer Agent (MTA) is used to provide routing functions that are necessary when communicating with Exchange 5.5 or other systems, such as those accessed through Connector for Lotus Notes or Connector for Novell GroupWise. Because the MTA is necessary for communicating with these other messaging systems in a hybrid environment, you should ensure that the Microsoft Exchange MTA Stacks service is running on every Exchange server on your network.

The MTA has two performance counters that can be used to determine how the MTA is functioning. The MSExchangeMTA object provides information on the bytes that have been transmitted and received using TCP/IP, X.25, and XAPI in messages and across the network. In addition to this, it also provides information on disk reads/writes, threads, and administrative connections. The MSExchangeMTA Connections object also provides counters that deal with the number of messages, the size of data in messages, and the number of associations needed to transfer messages over an X.400 connection.

When the Exchange Management Pack is imported into MOM, you can track events related to the MSExchangeMTA object, which will allow you to monitor the Microsoft Exchange MTA Stacks service. The categories related to MTA events are as follows:

- **Application Protocol Data Unit (APDU)**, which is used to track MTA send/receive information and communication between MTAs, which can indicate issues related to interoperability and conformance
- **Configuration**, which consists of parameters and problems related to MTA configuration files
- **Directory Access**, which provides information on events related to directory usage by the MTA
- **Interface**, which consists of elements related to communication between MTA components and MTAs
- **MTA Administration**, which allows administrative programs to access MTA queues and routing information
- **Operating System**, which consists of events related to the MTA's usage of Windows NT functions, such as the creation of threads or file operations
- **Resource**, which consists of events related to MTA resources
- **Security**, which deals with events related to security violation attempts

- **X.400 Service**, which deals with events related to the X.400 protocol, such as those for submission and delivery reports

Summary

Although the Exchange 5.5 Management Pack is still available for previous versions of MOM, it is important to realize that Exchange 5.5 is a legacy system, and should be upgraded to a newer version. As we saw, some support is available to connect to an Exchange 5.5 server in MOM 2005, but it is unlikely that even this level of support will continue in future versions of MOM.

Once you've installed a server on your network that uses a new version of Exchange, you can still access a legacy Exchange 5.5 server through the Microsoft Transfer Agent (MTA), which provides routing functions that allow communication with Exchange 5.5. This allows you to have a hybrid environment, such as when temporarily keeping an older server, in case information may be needed until it is decommissioned.

Although Exchange 5.5 is no longer supported by Microsoft, you can still acquire and import the Exchange 5.5 Management Pack for MOM 2000 or communicate with these servers in MOM 2005 using the Microsoft Transfer Agent. This provides some support to legacy systems that may reside on your network.

Solutions Fast Track

Managing Exchange 2000 and 2003

☑ Importing the Exchange Management Pack into Microsoft Operations Manager adds rules, interfaces, and other features into the MOM environment.

☑ The Configuration Wizard is a separate tool that can be installed. It will aid you in making configurations to Exchange.

☑ The Administrator Console is an interface that is used to configure MOM 2005 and the Exchange Management Pack. It allows you to view information about Exchange on the network.

☑ The Operator Console is an interface that is used to monitor the health of systems, identify potential problems, and provide recommended resolutions to various issues.

☑ The Product Knowledge Base in the Operator Console can be used to view technical information on solving known issues on an Exchange server. The Knowledge Base can be customized to add information that is specific to your company.

Monitoring Exchange 2000 and 2003

- ☑ Using the interfaces and rules available in Exchange Management Pack, you can monitor events and the server's health, as well as manage the availability of Exchange.
- ☑ Using reports available through the Exchange Management Pack, you can create documents that summarize information about Exchange.
- ☑ Rules imported with the Exchange Management Pack are used to run scripts and acquire data used for different views and reports. Many of these rules are configurable, and they will return an alert only when an event occurs or a counter reaches a value that you specify.

Managing and Monitoring Exchange 5.5

- ☑ Microsoft no longer supports Exchange 5.5, so newer versions of the Management Pack specifically for this system are no longer created.
- ☑ The Microsoft Transfer Agent is used to provide routing functions that are necessary when communicating with Exchange 5.5 or other systems. It enables MOM 2005 to monitor and communicate with Exchange 5.5.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: I am using the Operator Console and see an event number. How can I get more information on this event?

A: Click the **Product Knowledge Base** tab in the Operator Console to view details on the event, and in some cases, how to deal with it.

Q: Why do some of the rules for monitoring counters and events seem to deal with the same issue?

A: Some of the counters do deal with similar events, but are different to indicate the significance of an event. For example, although one rule may deal with low disk space, another will indicate that disk space is critically low. Low disk space is inconvenient,

but if there is no disk space available, then transaction logs or other information may be extremely difficult to recover.

Q: I've imported the Exchange Management Pack, but can't find the Configuration Wizard. How can I tell if it's been installed?

A: The Configuration Wizard is a separate tool that's found in the Tools folder on the MOM CD. It is not installed when the Exchange Management Pack is imported.

Q: I have just imported the Exchange Management Pack and tried to modify a number of rules. Now certain rules aren't being applied and notifications aren't being sent. What should I do?

A: Reimport the Exchange Management Pack. Rules that you modified, enabled, or disabled will be overwritten when you import the Exchange Management Pack. Because you've recently imported it for the first time and then made the changes, this should revert it to the state before your changes were made.

Chapter 7

Managing SQL Server 2000

Solutions in this chapter:

- **Managing SQL Server 2000**
- **Monitoring SQL Server 2000**
- **Performing SQL Server 2000 Operations**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

The SQL Server 2000 database where your MOM 2005 database is stored is one of the most important systems in your enterprise environment. The Microsoft SQL Server Management Pack provides you with a proactive and reactive way to both monitor and maintain your SQL Server 2000 systems. Ensuring availability through both local and remote connectivity checks, monitoring your configurations, and collecting data concerning your system performance through default thresholds allow for enterprise level monitoring that helps to ensure system integrity and health. This chapter will cover these things as well as how to use the management pack to manage and monitor SQL Server 2000 in your enterprise to take advantage of these resources.

Managing SQL Server 2000

First, make sure that you have a good understanding of the MOM 2005 monitoring features. Make sure you're also familiar with how to deploy management packs as discussed in Chapter 4. It will also help if you can manage and administer SQL Server 2000 and have a working knowledge of databases and Transact-SQL. Basically, this management pack allows you to monitor key data points to ensure the availability of your SQL Servers and related components as well as maintain a reliable day-to-day operation of your SQL Server instances.

Overview of the SQL Server 2000 Management Pack

So just what will the SQL Server 2000 Management Pack do for you? First, it provides enterprisewide configuration support, monitors both service and database availability and health, oversees both local and remote database connectivity, monitors database space, verifies service pack compliance, and monitors blocked system process ids just to name a few. Let's take a closer look at these and other capabilities of the SQL Server 2000 Management Pack.

As we said, the SQL Server 2000 Management Pack provides Enterprise level configuration support. It can monitor not only multiple instances of SQL Server 2000, but it also monitors both Active/Passive and Active/Active cluster configurations and SQL Server 64-bit edition instances. It can monitor configurations and provide information on inconsistencies in the enterprise for each database.

This management pack also monitors both service and database availability and health. This includes the availability of the SQL Server, the SQL Agent services, and

the Full Text Search service. It also provides for alerts on all databases in suspect and emergency states.

SQL Server Management Pack also oversees both local and remote database connectivity by providing monitoring for all database connectivity issues. This includes configuration and port bind errors, as well as protocol problems and corrupt system databases. The management pack also has the ability to connect to the database remotely so as to simulate the client experience testing database response time with custom TSQL queries.

Monitoring database space also is accomplished through enterprise adjustable warning and error thresholds for logs and databases, system databases, the Tempdb, and all user databases. The SQL Server Management Pack is file- and file–group-aware, and intelligent free space monitoring monitors the remaining space in all databases and transaction logs.

The SQL Server management pack verifies service pack compliance by checking all computers running SQL Server to see if they are running the minimum service pack that you have defined. It then generates success and failure alerts for auditing, and the Service Pack and Compliance Reports display the various version, build, and service pack level for each SQL Server in your MOM 2005 environment.

It also monitors blocked processes based on a blocking duration threshold time. Various alert details include blocked SPID, blocked by SPID, Program Name, Block Duration, Login Name, Database Name, and Resource. There's also a topped blocked report that allows further drilldown on data including top blocking users, application, and average blocking time.

Monitoring both replication and backups and jobs also is accomplished using the SQL Server management pack. The health of SQL Server replication and alerts on replication failures are provided. Also, failed SQL Agent jobs, backups, and notifications are reported as well as any job corruption, SQL Mail problems, full and incremental/differential backups, and any restore errors. It also allows for the monitoring of long-running agent jobs by measuring the run-time of the job in real-time and comparing that with a predetermined threshold that has been designated.

Finally, this management pack provides information concerning server performance such as disk response time, SQL process CPU use, deadlocks, user connections, and schema-specific performance problems.

Dependencies

The SQL Server 2000 Management Pack has some features that are going to require you to install additional components for it to operate properly. Those two components are the SQL Server Administration Tools and the Windows Base Operation System Management Pack.

Two functions of the SQL Server 2000 Management Pack require the SQL Server Administrator Tools to be installed on the MOM Operator Console computer. Those two functions are the SQL Server Query Analyzer and the SQL Server Profiler. You'll need to install the SQL Server Administration Tools on any MOM 2005 Operator Console computers where these functions will be used.

Performance counter collection in the Windows Base Operating System public views of the SQL Server 2000 Management Pack is dependent on the Windows Base Operating System Management Pack. Without it, those public views in the SQL Server 2000 Management Pack may not display performance data.

SQL Server 2000 Management Pack Components

The SQL Server 2000 Management Pack components include monitoring scenarios that support enterprise configuration support, service and database availability and health, database connectivity, remote connectivity, database space, service pack compliance, configuration monitoring, blocked processes, replication monitoring, long-running agent jobs, security monitoring, backups and jobs, and server performance. Table 7.1 provides a breakdown of the details for each scenario.

Table 7.1 Management Pack Monitoring Scenarios

Scenario	Details
Enterprise configuration support	■ Multiple instance aware ■ 100% cluster aware (both Active/Passive and Active/Active) ■ Monitors SQL Server 64-bit edition
Service and database availability and health	■ Availability of SQL server ■ SQL agent services ■ Full text search service ■ Alerts on databases in suspect and emergency states
Database connectivity	■ Local connectivity ■ Database connectivity issues ■ Port bind errors ■ Configuration errors ■ Protocol problems ■ Corrupt system databases
Remote connectivity	■ Connects to SQL server remotely to simulate the client experience ■ Tests database response time with custom TSQL query

Continued

Table 7.1 continued Management Pack Monitoring Scenarios

Scenario	Details
	■ Evaluates intermediate network connectivity ■ User-defined criteria ■ Query to execute ■ Database to query ■ Response time ■ Client computers
Database space	Intelligent free space monitoring monitors the remaining space in all databases and transaction logs ■ Files and file groups aware ■ Enterprise adjustable warning and error thresholds ■ Separate thresholds for: Logs and databases System databases Tempdb User databases
Service pack compliance	■ Check computers running SQL server for compliance with a minimum, and user-defined, service pack, or hotfix level ■ Generate success and failure alerts for auditing ■ Service pack and compliance reports displaying version, build, and service pack levels
Configuration monitoring	■ Alert on configuration inconsistencies in your enterprise for each database, including: Auto close Auto create stats Auto shrink Auto update stats Cross database chaining Torn page detection
Blocked processes	■ Monitors blocking system process IDs (SPIDs) based on a blocking duration threshold time. Alert details include:

Continued

Table 7.1 continued Management Pack Monitoring Scenarios

Scenario	Details
	Blocked SPID Blocked by SPID Program name Block duration Login name Database name Resource ■ Topped block report allows further drilldown on data including top blocking users, application, and average blocking time
Replication monitoring	■ Monitors the health of SQL server replication and alerts on replication failures
Long-running agent jobs	■ Job run-time measured in real-time and compared against a predetermined threshold
Security monitoring	■ Monitors SQL Server security and audit events: Denied administrative functions Single user mode startup License compliance Shutdowns Configuration problems Collection of audit data Successful and failed logins Trusted and untrusted connections
Backups and jobs	■ Failed SQL Agent jobs ■ Job corruption ■ Failed notifications ■ SQL mail problems ■ Failed backups ■ Incremental/differential backups ■ Restore errors
Server performance	■ Poor disk responses ■ Excessive SQL process CPU use ■ Deadlocks ■ Excessive user connections ■ Schema specific performance problems

Several of these scenarios are configurable and some even require configuration before they are usable. Those that are configurable include:

- SQL Server Service Availability
- Database Space Monitoring
- Remote Connectivity Checking
- Service Pack Compliance
- Database Health Monitoring
- Database Configuration Monitoring
- Block Analysis
- Long Running Agent Jobs
- Excluding Agent Jobs from Monitoring
- Excluding Databases from Monitoring
- Performance Thresholds
- SQL Replication Performance Collection

Of this group, six require configuration before they can be used. Those requiring configuration are:

- Remote Connectivity Checking
- Service Pack Compliance
- Database Configuration Monitoring
- Excluding Agent Jobs from Monitoring
- Excluding Databases from Monitoring
- SQL Replication Performance Collection

Let's take a look at how you would configure two of these, one with optional configuration and one with required configuration. Database Space Monitoring configuration is optional. Service Pack Compliance configuration is required.

Database Space Monitoring is turned on by default. You can check this in the Administrator Console under SQL Server 2000\State Monitoring and Service Discovery\Event Rules\SQL Server Space Analysis. You can modify the threshold values used by the event rules to trigger warning and error events. By default, no modification is necessary.

SOME INDEPENDENT ADVICE

If you decide to modify these thresholds, you should work with your database administrators to determine what your warning and error threshold levels should be.

To customize database space analysis monitoring:

1. Open the MOM 2005 Administrator console and navigate to the SQL Server Space Analysis event rule.
2. Right-click the rule and choose properties from the drop-down menu. Now click the **Response** tab.
3. In the Script parameters box, highlight the SQL Server 2000 Space Analysis script and then click **Edit**.
4. Change a script parameter by highlighting the parameter and clicking **Edit Script Parameters**.
5. After modifying the script responses click **OK**. Click **OK** again and then click **Apply**.
6. After you have modified the script responses, commit the configuration changes to apply the changes to agent computers.

Service Pack Compliance requires a certain level of configuration. Although enabled by default, the specific service pack or hot fix level must be set by you. To configure service pack monitoring:

1. Open the MOM 2005 Administrator console and navigate to SQL Server 2000\SQL Server 2000 Health and Availability Monitoring\Event Rules.
2. Right-click the SQL Server Service Pack compliance rule and click **Properties** from the drop-down menu. Click the **Response** tab.
3. Highlight the SQL Server 2000 Service Pack Compliance script and click **Edit**.
4. In the Script Parameters box, choose AlertOnAll and click **Edit Script Parameters**.
5. To receive success version compliance alerts type **True** in the Value box and then click **OK**.

6. To modify the version string, in the Script parameters box choose **VersionString** and click **Edit Script Parameters**.
7. In the value box enter the SQL Server version number that applies to your environment and then click **OK**.
8. To generate success alerts in addition to failure alerts, in the Script parameters box, select **AlertOnAll** and then click **Edit Script Parameters**.
9. Change the value to **True** and click **OK**.
10. After modifying script responses, click **OK**, then apply, and then click **OK** again.
11. After changing the script responses, commit the configuration changes to apply the changes to agent computers.

Importing the SQL Server 2000 Management Pack

Managing SQL Server 2000 with MOM 2005 starts with deployment of the MOM 2005 Microsoft SQL Server Management Pack. Installing the management pack is a relatively simple process that we covered in Chapter 4. We'll look at a new deployment first and then cover upgrade deployments.

For a new deployment, open the MOM 2005 Administrator Console. As we have suggested previously, it's a good idea to develop a specific procedure that you'll follow every time you import a management pack into your MOM 2005 Management group. This will assure that the installations are performed correctly and in the same manner.

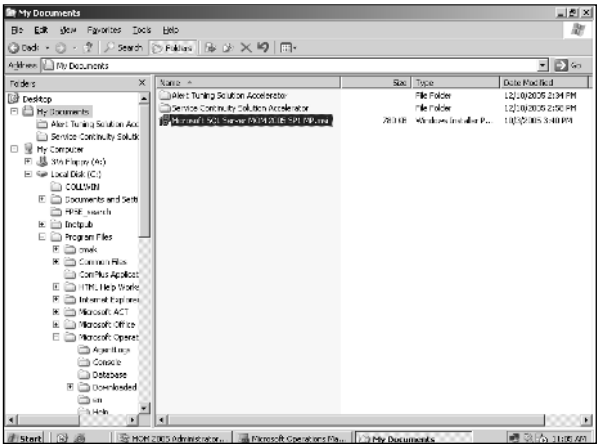
BEST PRACTICES ACCORDING TO MICROSOFT

You really should import any management pack you plan on using into your test environment first and not directly into your production environment. This allows you to learn how the management pack operates and what other configuration and permissions might be required for the management pack to perform correctly before you put it into a live production system.

Installation of a management pack is a simple process, as was explained in Chapter 4, but we will go over it again here as a reminder. First, if you've downloaded the management packs from Microsoft you will need to install them before you can import them.

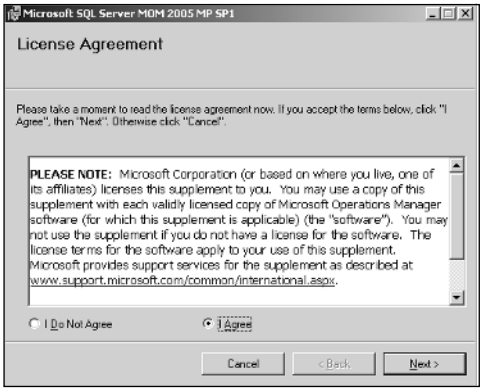
Find where you downloaded the MSI file to, as seen in Figure 7.1, and double-click it.

Figure 7.1 Locate the MSI File Where You Downloaded It



Agree to the license agreement, as seen in Figure 7.2, and click the **Next** button.

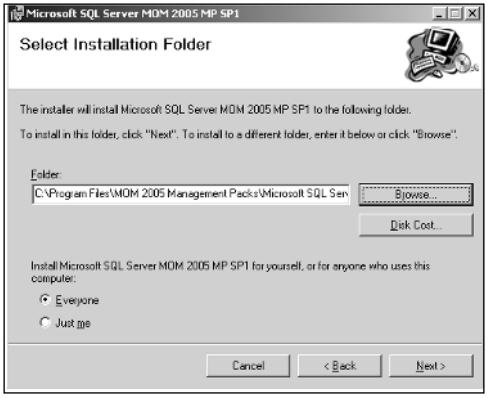
Figure 7.2 Agree to the License Agreement



As seen in Figure 7.3, you now need to choose your installation folder. Pay special attention to the default folder because you will need it later. Choose if you want everyone to have access to the management pack or just you and then click **Next**.

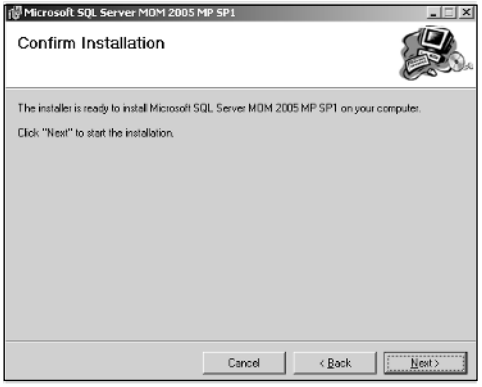
In most cases, since you will not be the only administrator on this machine, you will want to use the default **Everyone** option.

Figure 7.3 Choose Your Installation Folder



The next dialog window, as seen in Figure 7.4, shows that you are ready to begin the management pack installation. Click the **Next** button.

Figure 7.4 Confirm the Installation of the Management Pack



The installation of the management pack will complete, as seen in Figure 7.5. Click the **Close** button.

Your next step is to open the Administrator Console, as seen in Figure 7.6, and choose Import Management Packs.

Figure 7.5 The Installation Is Complete

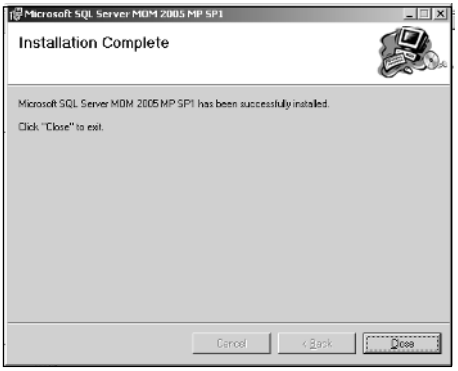
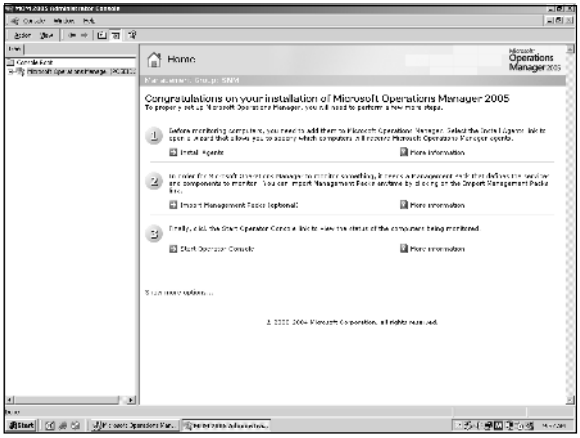
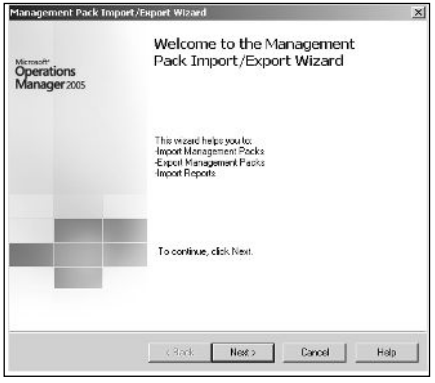


Figure 7.6 Choose Import Management Packs



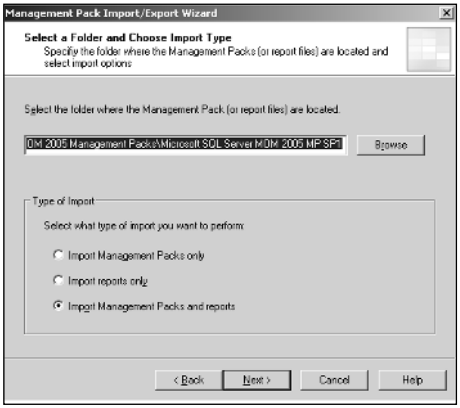
The Welcome screen for the Import/Export wizard will appear as shown in Figure 7.7. Click the **Next** button on this dialog window.

Figure 7.7 Welcome to the Import/Export Wizard



The default selection on the Import or Export Management Packs dialog window is set to Import Management Packs and/or Reports as seen in Figure 7.8. Accept this default and click the **Next** button.

Figure 7.8 Time to Find the Folder Where the Management Pack Was Stored



On the Select a Folder and Choose Import Type dialog window, as seen in Figure 7.8, click the **Import Management Packs and reports** under Types of Import and then click the **Browse** button.

In the Browse for Folder dialog window, as seen in Figure 7.9, navigate to the folder where the management pack is located (remember, we told you that you would need to remember where it was installed) and then click the **OK** button. When this dialog window disappears, click the **Next** button on the underlying dialog window to continue (see Figure 7.10).

Figure 7.9 Navigate to the Folder Where Your Management Pack Is Located

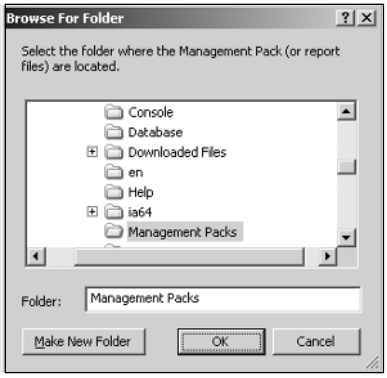
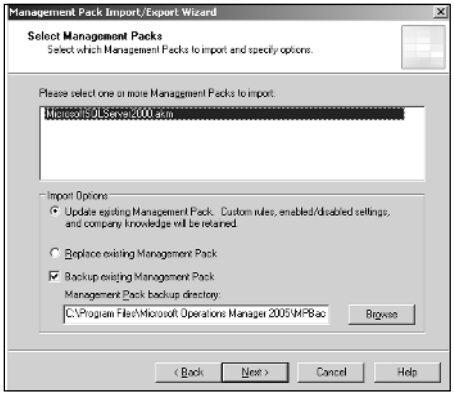
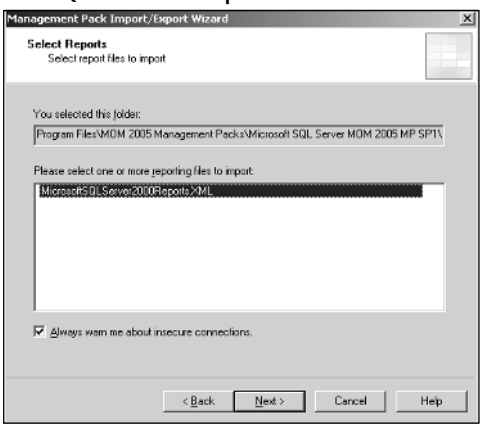


Figure 7.10 Select the SQL Server 2000 Management Pack



On the Select Management Packs dialog window, as seen in Figure 7.11, choose the SQL Server 2000 Management Pack and select an import option. It's a good habit to get into to always choose **Update Existing Management Pack**. This will retain any custom rules, settings, and company knowledge that you may already have entered into your MOM 2005 environment. You also probably want to make sure the **Backup Existing Management Pack** option is checked in case you need to restore it at a later point in time. When you have changed any options you may need to change click the **Next** button.

Figure 7.11 Select the SQL Server Reports File You Want to Import



In the Select Reports dialog window, as seen in Figure 7.11, select the SQL Server 2000 reporting file and then click the **Next** button.

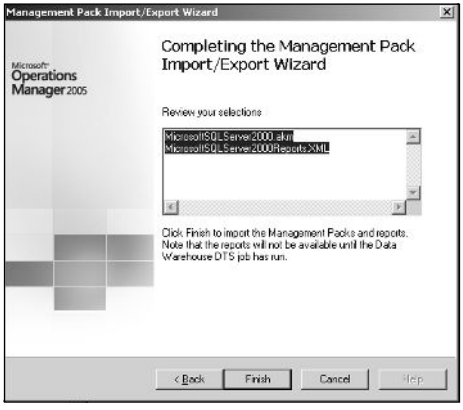
If you installed the SQL Server Reporting Services according to our instructions in Chapter 4, you'll remember that the instructions detailed the differences between

installing on a test server and on a production server. If you followed our instructions and set up this installation as a test server then you will see the dialog window seen in Figure 7.12. Basically, for a test server there is really no need to use Secure Socket Layer (SSL) for the connection. For a production server, however, you would want to make sure that you were using SSL and would want to go back and correct this situation. For our test purposes here, simply click the **Continue** button to move on.

Figure 7.12 You May Receive a Secure Socket Layer Warning

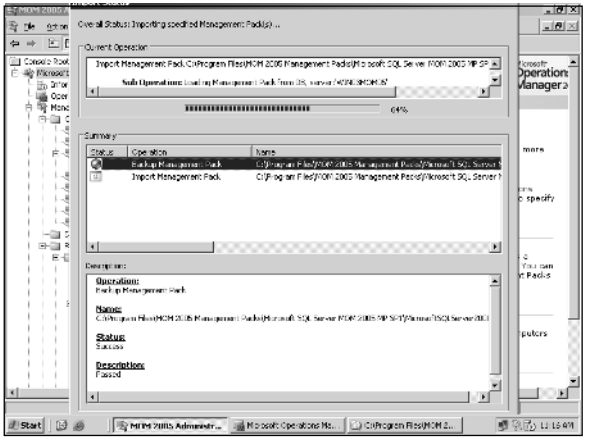
Finally, click the **Finish** button in the next dialog window, as seen in Figure 7.13, to complete and close the wizard.

Figure 7.13 Completing the SQL Server 2000 Management Pack Installation



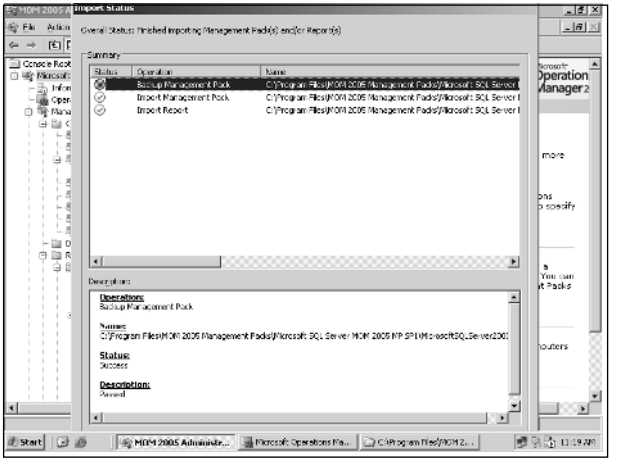
As seen in Figure 7.14, the import process may take a few minutes. The first step will be to back up the previous management pack, if there is one. Next it will import the new management pack and then it will import the new reports. The wizard will keep you informed of each step along the way.

Figure 7.14 The Import Process May Take a Few Minutes



When the wizard is complete, as seen in Figure 7.15, simply press **Enter** to close the wizard.

Figure 7.15 Both the Management Pack and the Reports Imported



After importing the management pack, the new rules can be viewed immediately in the MOM 2005 Administrator console, as seen in Figure 7.16, and the views can be viewed immediately in the MOM 2005 Operator Console, as seen in Figure 7.17.

Figure 7.16 The New Rules in the MOM 2005 Administrator Console

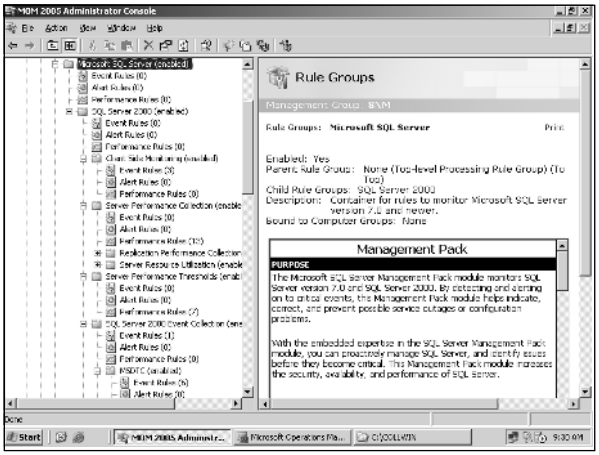
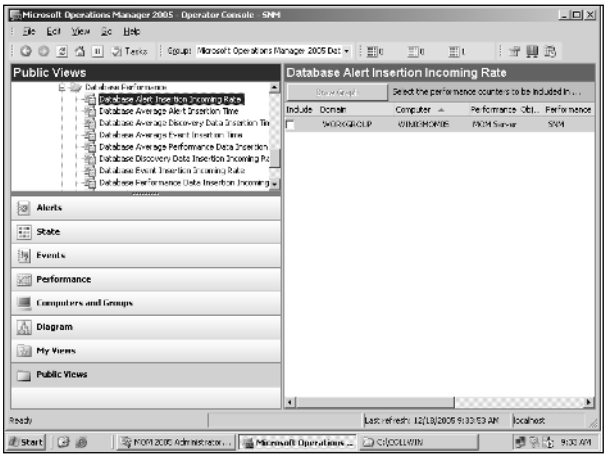


Figure 7.17 The New Views in the MOM 2005 Operator Console



Upgrading can be accomplished from the SQL Server 2000 Management Pack Refresh for MOM 2000 SP1. If you still have SQL Server 7 instances that need to be monitored, you can install the SQL Server 2000 Management Pack Refresh for MOM 2000 SP1 and then upgrade to the SQL Server 2000 Management Pack for MOM 2005. If you already have SQL Server 2000 Management Pack Refresh for MOM 2000 SP1 installed for monitoring SQL Server 7, then after upgrading you will continue to have the same level of support as you have had previously.

Keep in mind that after the upgrade you will need to reset the values for certain processes. Those processes include:

- SQL Server Service Availability

- Database Space Monitoring
- Database Health Monitoring
- Performance Rule Customization

The SQL Server Service Availability process needs the Full Text Search service monitoring to be enabled if applicable. By default, SQL Server Service Availability is enabled but the script parameter for monitoring the Full Text Search is disabled by default. For database monitoring you'll need to reset the database size values that trigger the warning and error events. For database health monitoring reset the list of high severity databases if applicable. Finally, for performance rule customization, reset any customizations that you've made to any performance rules.

Remember that any customizations you've made to Company Knowledge and any changes you've made to the enabled or disabled state of rules will be maintained after the upgrade. Any changes you made to existing rules in a previous version of the SQL Server Management Pack will need to be copied into a dedicated management pack before the upgrade process. You also, as we have said previously, should perform a full database backup before you perform the upgrade of the management pack.

Best Practices According to Microsoft

The Import Management Pack wizard in MOM 2005 allows you to perform a backup of the previous version of the SQL Server Management Pack. It is best to leave the **Backup existing Management Pack** check box selected. That way if you need to you can always revert to the previous management pack.

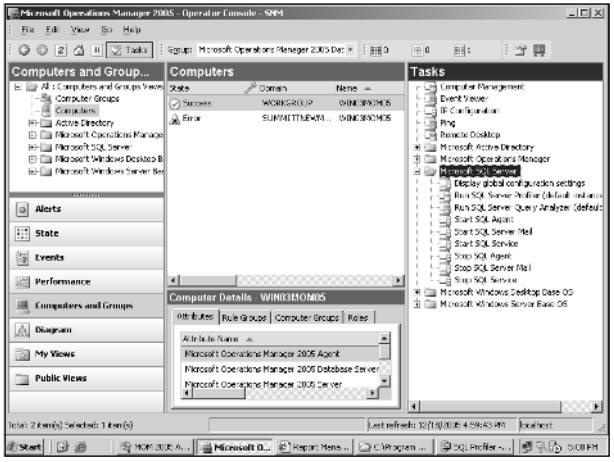
Performing Management Tasks

We'll discuss tasks more in depth later in this chapter, but at this point it's a good idea to become somewhat acquainted with the tasks and what they do. There are seven main tasks that are handled by the SQL Server Management Pack. These tasks are available in the tasks pane of the Operator console as seen in Figure 7.18:

- Display global configuration settings
- Run SQL Server Profiler against the default instance
- Run SQL Server Query Analyzer against the default instance
- Stop SQL Mail

- Start SQL Mail
- Start and Stop SQL Agent
- Start and Stop SQL Service

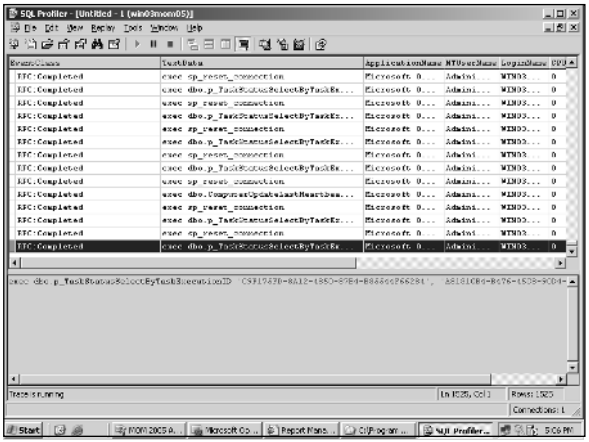
Figure 7.18 Management Tasks



The Display global configuration settings task executes a SQL Server stored procedure called SP_CONFIGURE against a specific SQL Server instance or a combination of selected instances. This task is aware of the instance it is being directed against.

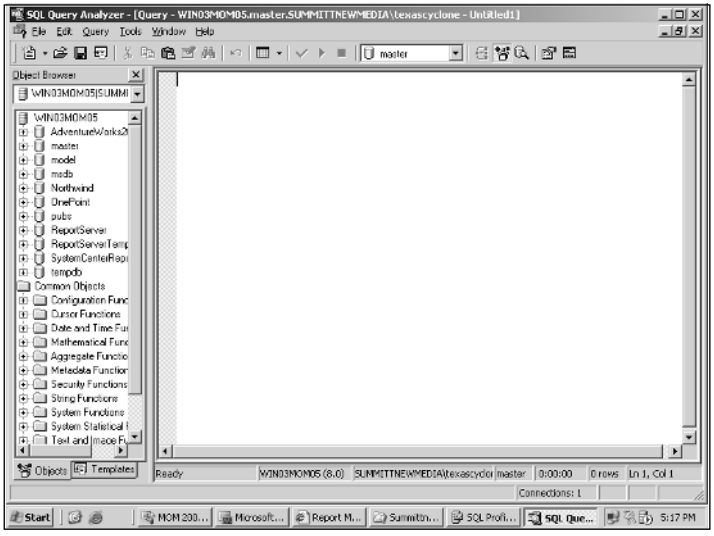
The Run SQL Server Profiler against the default instance task, as seen in Figure 7.19, does exactly what it says. The SQL Server Profiler is run against the default SQL Server instance.

Figure 7.19 You Can Run the SQL Server Profiler from the Operator Console



The same is true for the Run SQL Server Query Analyzer against the default instance task. It executes the SQL Server Query Analyzer and runs it against the default SQL Server instance as seen in Figure 7.20.

Figure 7.20 You Can Also Run the SQL Server Query Analyzer



The Stop and Start SQL Mail tasks execute the SQL Server stored procedures SP_STOPMAIL and SP_STARTMAIL against all SQL Server instances. These tasks are not supported, however, in the 64-bit version of this management pack.

Finally, as with the previous tasks, the Start and Stop SQL Agent and Start and Stop SQL Server tasks do just what they say. They start and stop the SQL Server Agent and SQL Server Service for all installed SQL Server instances in the MOM 2005 environment. Again, both of these tasks are instance-aware.

SQL Server Management Views

There are four main groupings of SQL Server Management Views. Those groupings are:

- Standard default views
- Server resource utilization views
- SQL Server health monitoring views
- SQL Server utilization and performance views

The standard default views are also called the public views and require no additional configuration. The views that are available in this grouping are shown in Figures 7.21 through 7.28

Figure 7.21 Alerts

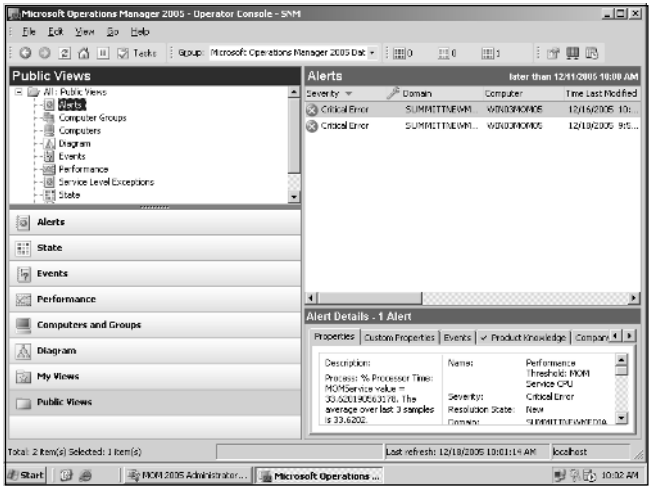


Figure 7.22 Computer Groups

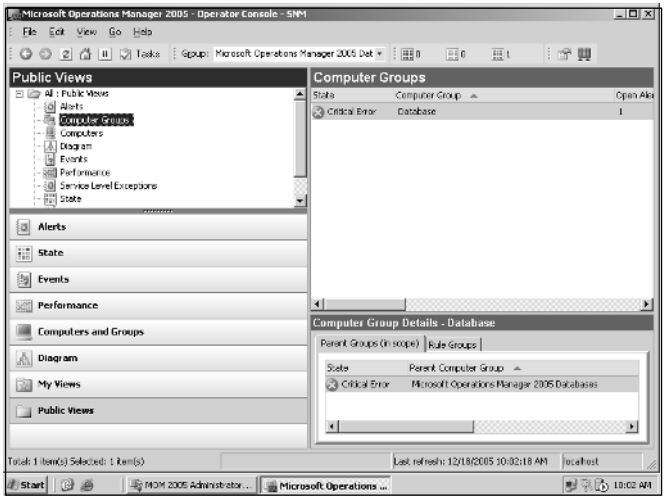


Figure 7.23 Computers

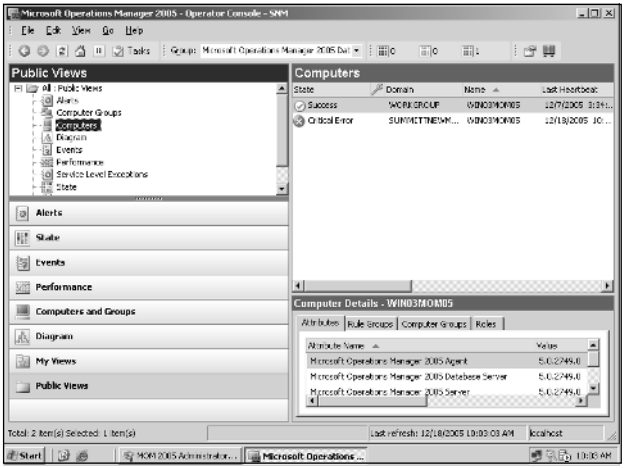


Figure 7.24 Events

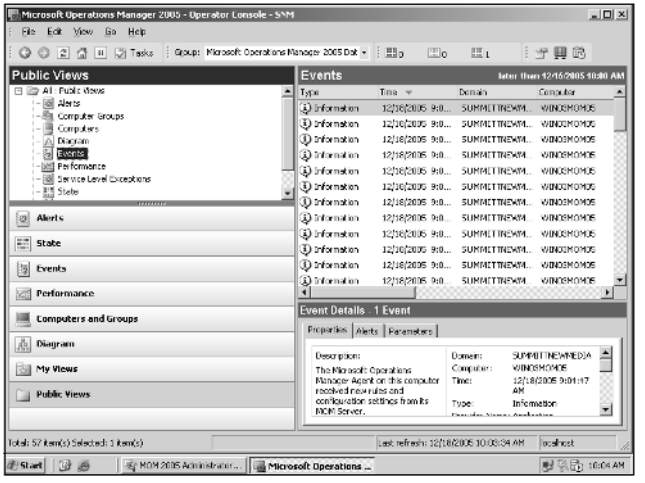


Figure 7.25 Performance

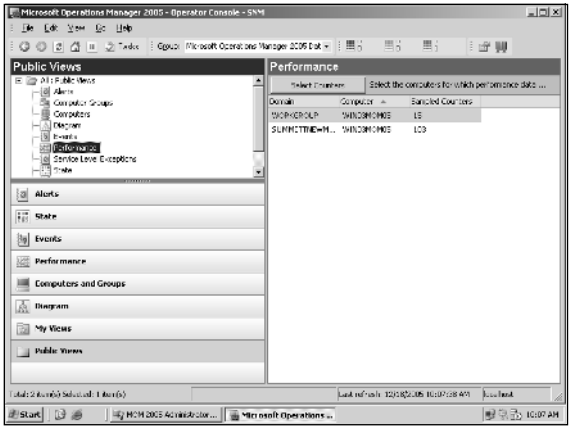


Figure 7.26 Service Level Exceptions

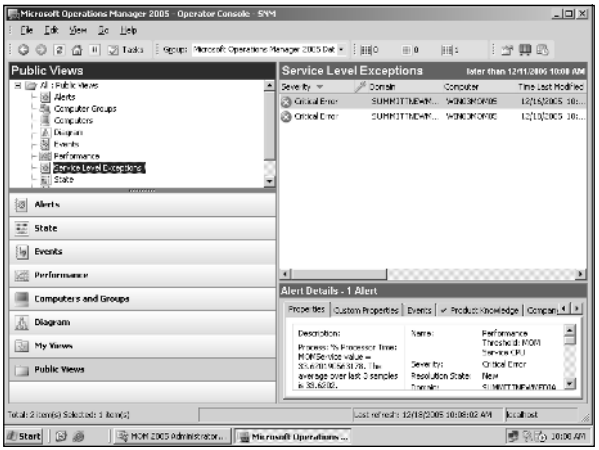


Figure 7.27 State

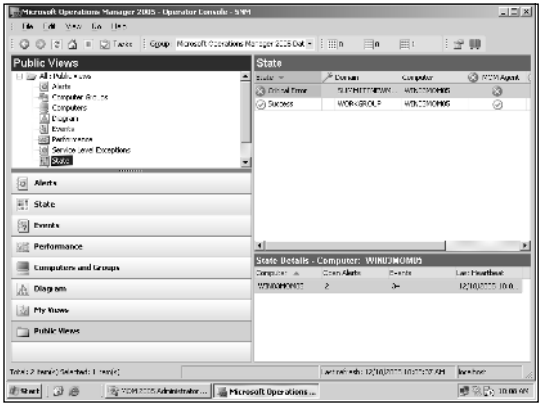
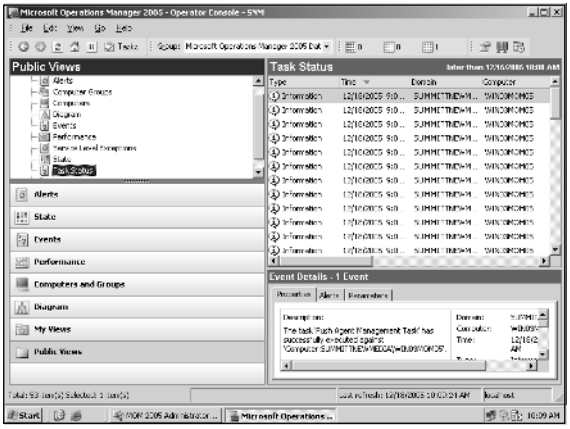


Figure 7.28 Task Status



The Server Resource Utilization Views include views that provide information on the CPU usage, disk capacity, disk performance, memory usage, and network usage. Many of these views also require that the Microsoft Windows Server Base Operating System Management Pack be installed. The views that provide information concerning CPU usage are:

- % CPU: MOM process
- % CPU: SQLAGENT process
- % CPU: SQLMANGR process
- % CPU: SQLSERVR process
- Context switches per second
- Processor queue length
- Total % CPU usage

Disk capacity information is provided through two views:

- % Free space
- Free megabytes

Disk performance is provided via four views:

- Average disk queue length
- Current disk queue length
- Disk read and write latency

- Disk reads and writes per second

For Memory usage there are five views:

- Memory: Page reads per second
- Memory: Page writes per second
- Memory: Pages per second
- Memory: Pool nonpaged bytes
- Memory: Pool paged bytes

And finally, Network usage is provided via three views:

- Bytes received per second
- Bytes sent per second
- Bytes total per second

The third grouping provides SQL Server Health Monitoring views. Information in these views is provided on SQL Agents, SQL Server backups, SQL Server databases, SQL Server Replication, SQL Server Replication\Distributor, SQL Server Replication\Log Reader, SQL Server Replication\Merge, and SQL Server Replication\Snapshot. The views that will provide this information are:

- Failed SQL agent jobs
- Failed SQL backups
- Database free space alerts
- Database health alerts
- Transaction log free space alerts
- Replication agents running
- SQL Server 2000 replication servers
- Delivered commands per second
- Delivered transactions per second
- Conflicts per second
- Downloaded changes per second
- Uploaded changes per second

The fourth and final grouping provides information concerning SQL Server Utilization and Performance. The available views include:

- Active transactions
- Average wait time per millisecond
- DBCC logical scan bytes per second
- Full scans per second
- Lock blocks
- Lock timeouts per second
- Log cache reads per second
- Log truncations
- Logins per second
- Memory grants pending
- Mixed page allocations per second
- Page writes per second
- Pages allocated per second

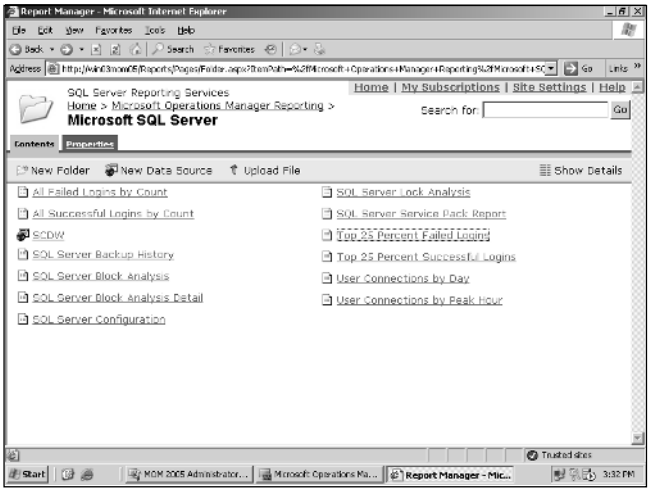
Overview of SQL Server 2000 Reports

There are twelve basic reports that are included in the Microsoft SQL Server Management Pack. Those twelve reports, as seen in Figure 7.29, are:

- All failed logins by count
- All successful logins by count
- SQL Server backup history
- SQL Server block analysis
- SQL Server block analysis and detail
- SQL Server configuration
- SQL Server lock analysis
- SQL Server service pack
- Top 25 percent failed logins
- Top 25 percent successful logins

- SQL Server user connections by day
- User connections by peak hour

Figure 7.29 Basic SQL Server 2000 Reports



Clicking **All Failed Logins by Count** will display all the collected failed login data within the specified date range. This includes any cumulative totals for failed login attempts and type. Clicking **All successful Logins by Count** provides a count of all successful logins. This screen will display a report that lists the number of successful logins and the types of connections for each user.

Clicking the **SQL Server Backup History report** provides a listing of all backups of all instances on a server and includes the ability to drilldown to a specific value for more detailed information.

The SQL Server Block Analysis report provides a summary of all blocking incidents for a specified SQL Server. This report includes the names of programs that are affected, the total number of blocks, and the average block time in seconds for each database on the server. Similarly, the SQL Server Block Analysis and Detail report provides detailed data on each of the blocking incidents on the specified SQL Server. This report includes the name of the database, the program, the block duration, the login name, the resource, the blocked SPID, and the blocking SPID for each blocking incident.

The SQL Server Configuration report provides details concerning the configuration of all SQL Server instances and their databases on a server. The SQL Server Lock Analysis report provides a display of the total number of deadlocks, lock requests, and lock waits on all instances on a specified server. The SQL Server

Service Pack report provides the version and service pack level of all monitored SQL Server instances.

The Top 25 Percent Failed Logins and Top 25 Percent Successful Logins reports chart the top 25 percent of users with failed or successful login attempts respectively. These reports are for a given time period and include cumulative totals for each user. Finally, the SQL Server User Connections by Day and the User Connections by Peak Hour reports provide listings of the number of SQL Server user connections over a specified data range and over a specified date range and peak hour time range in a graphical format, respectively.

Generating Reports

By default, your reports are going to be empty because no data is collected for reporting. That keeps your database from growing out of control. If you want or need to enable reporting, the processing rules that collect the data for reports have to be enabled. This section lists the processing rules that need to be enabled and includes setup for the following reporting scenarios:

- Reporting for clustered databases
- Reporting for named instances on SQL Server 2000

For SQL Server 2000, the processing rules that collect data for reporting are listed at:

- \SQL Server 2000\SQL Server 2000 Report Collection Rules\Event Processing Rules
- \SQL Server 2000\SQL Server 2000 Report Collection Rules\Performance Processing Rules
- \SQL Server 2000\Server Performance Collection\Replication Performance Collection\Event Processing Rules
- \SQL Server 2000\Server Performance Collection\Replication Performance Collection\Performance Processing Rules

For SQL Server 7.0, the processing rules that collect data for reporting are listed at:

- \SQL Server 7.0\SQL Server 7.0 Report Collection Rules\Event Processing Rules
- \SQL Server 7.0\SQL Server 7.0 Report Collection Rules\Performance Processing Rules

You have to enable the associated processing rules in order to collect the data that is used by reports. Remember that not all reporting processing rules are available for both SQL Server 7.0 and SQL Server 2000. Another thing to remember is that report names in some processing rule groups are preceded by Report Collection.

Agentless Monitoring

The SQL Server 2000 Management Pack for MOM 2005 allows for the monitoring of agentless managed computers with the following monitoring features:

- State monitoring
  - Service discovery
  - Service availability
  - Database health
  - Space analysis
- Health and availability monitoring
  - Database configuration monitoring
  - Service Pack compliance
  - Long-running agent jobs
  - Block analysis
  - Replication monitoring
- Server performance threshold monitoring
- Server performance collection
- Remote connectivity

The management pack doesn't support the following features on those SQL Servers that aren't monitored with an agent:

- Event collection
- Tasks that start and stop SQL Server services
- Tasks that start and stop SQL mail

Performing SQL Server 2000 Operations

The SQL Server Management Pack will generate reports that display data over time and will present patterns that indicate possible problems. Even though many of the important problems that may exist in your database will not cause an alert, they will still need your attention from time to time. Going over the information provided in the reports allows you to take a proactive rather than a reactive stance by resolving this type of issue before it can generate an alert.

Best Practices According to Microsoft

- Review and prioritize all your alerts on a daily basis.
- Perform other tasks on a regular basis, depending on your particular situation.

Daily Tasks

The following tasks should be performed every day:

- Review all open alerts
- Verify that all servers running SQL Server are communicating with the MOM 2005 Administrator console
- Review all warning

In the MOM 2005 Administrator console, choose **Monitor** and then **All Open Alerts**. You need to review the new alerts according to a set priority. That priority is:

1. Service Unavailable errors
2. Critical errors
3. SQL Server scripts (such as SQL Server Service Availability and SQL Server Remote Connectivity)
4. Warnings
5. Informational messages

Warnings and informational messages are optional but occasionally you should go through these also just to make sure you are aware of the day-to-day operation of your systems.

SOME INDEPENDENT ADVICE

Remember that not all problems will be corrected in a day or less. Parts may need to be ordered or a server may need to be scheduled for a restart. Just make sure you note these alerts and make sure you address them in a timely manner.

If your servers running the SQL Server instances and the servers running MOM 2005 have a communication failure this will prevent you from receiving the alerts that you need to examine and resolve. You should make sure that you verify on a daily basis that all servers are communicating with the MOM 2005 Management Structure. This is simple. In the MOM 2005 Operator console click **Public Views** and navigate to All Public Views, Microsoft SQL: Server, Computers. In the Computers pane click the **Last Heartbeat** column. All the systems will be sorted by the last contact time. If the last contact time for any of your systems is greater than five minutes you need to find out why the two systems are not communicating.

Weekly Tasks

At least once a week, in addition to the tasks you perform on a daily basis, you need to review the following reports:

- SQL Server Configuration
- SQL Server Service Pack
- Top 25 Percent Failed Logins
- SQL Server Lock Analysis
- SQL Server Block Analysis
- SQL Server Backup History

Monthly Tasks

Once a month you should also include two other reports in your analysis. Those reports can be found under Capacity planning and trending and would be User Connections by Day and User Connections by Peak Hour.

Some Independent Advice

You know your system better than any consultant or book author. You also should review any other reports that you think are appropriate for your installation.

Other Tasks

As needed you should review all open alerts, check and verify that all managed computers are communicating, and use the SQL Server public views.

Summary

Managing SQL Server 2000 using MOM 2005 is a relatively simple task. All the tools are available to you in the Operator's Console. In this chapter we have walked through the installation and importing of the SQL Server 2000 Management Pack and discussed the various management tasks and views that are now available to you. We also pointed out specific dependencies that exist with the various management packs and how installing just one is not going to be enough in all cases.

Monitoring the day-to-day operations of the SQL Server database is made quick and easy using the rules and views that are available. Reports can be viewed that provide you insight into possible problems that can arise over time. Finally, we discussed the development of a daily, weekly, and monthly regiment and routine that is built around your environment's needs.

Solutions Fast Track

Managing SQL Server 2000

- ☑ The SQL Server 2000 Management Pack monitors service and database availability, connectivity, and health.
- ☑ The SQL Server 2000 Management Pack has some features that require the installation of additional components for it to operate properly. Those two components are the SQL Server Administration Tools and the Windows Base Operation System Management Pack.

- ☑ It's always a good idea to develop a specific procedure to follow when importing a management pack into your MOM 2005 Management group. This ensures that the installations are performed correctly and in the same manner.
- ☑ There are seven main tasks that are handled by the SQL Server Management Pack. These tasks are available in the tasks pane of the Operator console and include Display global configuration settings, Run SQL Server Profiler against the default instance, Run SQL Server Query Analyzer against the default instance, Stop SQL Mail, Start SQL Mail, Start and Stop SQL Agent, and Start and Stop SQL Service.
- ☑ There are four main groupings of SQL Server Management Views. These groupings are Standard default views, Server resource utilization views, SQL Server health monitoring views, and SQL Server utilization and performance views.

Monitoring SQL Server 2000

- ☑ Reports are going to be empty by default because no data has been collected for reporting. This keeps the database from growing out of control. To enable reporting, the processing rules that collect the data for reports have to be enabled.
- ☑ The SQL Server 2000 Management Pack for MOM 2005 allows for the monitoring of agentless managed computers with the following monitoring features: State monitoring, Health and availability monitoring, Server performance threshold monitoring, Server performance collection, and Remote connectivity.

Performing SQL Server 2000 Operations

- ☑ The following tasks should be performed every day: Review all open alerts, Verify that all servers running SQL Server are communicating with the MOM 2005 Administrator console, and Review all warnings
- ☑ At least once a week, in addition to those performed on a daily basis, review the following reports: SQL Server Configuration, SQL Server Service Pack, Top 25 Percent Failed Logins, SQL Server Lock Analysis, SQL Server Block Analysis, and SQL Server Backup History.

- ☑ Once a month include two other reports in your analysis: both of these reports can be found under Capacity planning and trending and would be User Connections by Day and User Connections by Peak Hour.
- ☑ On an as-needed basis, review all open alerts, check and verify that all managed computers are communicating, and use the SQL Server public views.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Where can I get the SQL Server 2000 Management Pack?

A: The SQL Server 2000 Management Pack comes with MOM 2005 along with the management packs for Microsoft Baseline Security Analyzer, Microsoft Exchange 2000 Server, Microsoft Exchange Server 2003, Microsoft Operations Manager 2005, Microsoft SMS 2003, Microsoft Windows Active Directory, Microsoft Windows Base Operating System, Microsoft Windows DNS, Microsoft Windows IIS, and Microsoft Windows Server Clusters.

Q: Where do I find the latest version of the SQL Server 2000 Management Pack?

A: The Management Pack catalog, located at www.microsoft.com/management/mma/catalog.aspx, provides a comprehensive list of all the management packs currently available for MOM 2005 including the most recent version of the one for SQL Server 2000.

Q: Can I use MOM 2005 and the SQL Server 2000 Management Pack to monitor more than one instance of SQL Server 2000?

A: MOM 2005 and the SQL Server 2000 Management Pack can monitor not only multiple instances of SQL Server 2000, but can also monitor both Active/Passive and Active/Active cluster configurations and even SQL Server 64-bit edition instances.

Q: What is the difference between installing a management pack and importing it?

A: When you download a new management pack from Microsoft it will come in the form of an MSI file. This must be installed first, before you can import it into MOM 2005. When you install the SQL Server 2000 Management Pack it will be installed by default in the C:\Program Files\MOM 2005 Management Packs\Microsoft SQL Server MOM 2005 MP SP1 folder. When you get ready to import it into MOM 2005 so that you can use the management pack, you have to point the imported files to this directory. So the act of installing puts the files on your computer but the act of importing makes them available for your use.

Q: What does it mean when it says that MOM 2005 with the SQL Server 2000 Management Pack is instance-aware?

A: The MOM 2005 SQL Server 2000 Management Pack will automatically detect, and then start monitoring and managing, only those applications that are present on the target computer. The term instance-aware means that MOM is able to identify various instances of applications installed on your server, and can even start managing those application instances. In other words, MOM 2005 with the SQL Server 2000 Management Pack can detect and monitor applications in SQL server, such as an SQL instance supporting an accounting application and another instance supporting a product ordering application.

Q: Is the SQL Server 2000 Management Pack all I need to install or are there other management packs and tools that need to be installed for the various views, tasks, and reports to provide me with the information I need?

A: There are several features of the SQL Server 2000 Management Pack that require additional components be installed in order for it to work correctly. Make sure that the SQL Server Administration tools are installed on the same computer as the MOM 2005 Operator Console. You will also need to install the Windows Base Operating System Management Pack because the Windows Base Operating System public views in the SQL Server 2000 Management Pack are dependent on it for performance counter collection.

Q: I've installed everything like it says but I still can't see any information. What have I done wrong?

A: Nothing. You just need to have patience. The SQL Server 2000 Management Pack collects service discovery data every eight hours by default. Much information about the SQL Server 2000 instance might not be available for up to eight hours after the management pack is deployed. Also, the reporting component of MOM 2005 gets its information from a nightly DTS job that transfers information from the MOM 2005 database to the MOM 2005 Reporting database. Don't expect to have any useable data until after eight hours and the nightly DTS job has completed.

Q: Do I get the same kind of views, tasks, and reports if I'm using the MOM 2005 Workgroup Edition?

A: The MOM 2005 Workgroup Edition does not allow for the Reporting Service as with the Standard version so you won't get the reports as with the standard version. SQL Server 2000 Management Pack does comes with MOM 2005 Workgroup Edition, as does Microsoft Baseline Security Analyzer, Microsoft Exchange 2000 Server, Microsoft Exchange Server 2003, Microsoft Operations Manager 2005, Microsoft SMS 2003, Microsoft Windows Active Directory, Microsoft Windows Base Operating System, Microsoft Windows DNS, Microsoft Windows IIS, and Microsoft Windows Server Clusters Management Packs.

Chapter 8

Managing Microsoft Active Directory

Solutions in this chapter:

- **Managing Network Services**
- **Managing Active Directory Services**
- **Managing Group Policy**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

In almost every Microsoft Windows shop, Active Directory 2000 or 2003 is being used. Because of this central position in the network, not only its availability but also its performance and policy processing should be monitored. Active Directory, however, is only a small part of the infrastructure of your network. In addition to discussing Active Directory (AD) in this chapter, we will also address the most common network services found in an IT enterprise.

Managing Network Services

As Microsoft continues to build its management pack offering, you'll be able to expand your MOM infrastructure further and further. Already, Microsoft has released a number of small, easy-to-install management packs, enabling you to monitor even the most remote and dusty corners of your network.

You might think there's no need to monitor these areas because the Domain Name Service (DNS) server supposedly "runs like a charm and never fails." Although this can be true, there's no guarantee it will perform this way for another 10 years. If you import the management pack, however, you can trust that its components will work as planned—and if they fail, you'll be notified.

Best Practices According to Microsoft

Before importing the Active Directory Management Pack, be sure to load the DNS and Windows server base OS management pack. Otherwise, the AD Management Pack won't be able to determine the role of the server in the network, and it will fail to work correctly.

Some Independent Advice

Using MOM gives you the power to know what's going on in the network. If you're planning to buy new software for backups and restorations, keep in mind that you're also using MOM in your environment. Check if there's a MOM Management Pack to support the application. This way you can keep your central point of operation management.

If you think about it, there are a lot of network services depending on each other to work correctly. For example, the DHCP service depends on Active Directory to be authorized. If it's unable to check the authorization, it will shut down. Or an even better example: Active Directory depends on the DNS servers. If there are no DNS servers available, Active Directory isn't able to function.

This makes network services essential when it comes to providing good services to end users.

Managing DNS

Microsoft Windows 2000/2003 (as well as the upcoming Vista) operating systems are DNS based. This means that all name resolving is done using DNS. Even if your system is searching for the domain controllers, the DNS service is queried on the SRV records to get the LDAP location, thereby making DNS by far the most important core network service in your network.

If you're importing the AD Management Pack, the script in the pack is heavily dependent on the DNS services. It is a Microsoft best practice to first import the DNS Management Pack.

Depending on the DNS infrastructure configuration, several types of configurations are available. If possible, spread the DNS servers across two or more management servers and be sure to monitor all DNS servers in your network. This is essential for a successful implementation of the management pack.

Depending on the DNS server configuration, there are several recommended methods to monitor the DNS environment. However, these configurations go beyond the scope of this book because they are mostly related to redundancy in monitoring. As always, the DNS Management Pack requires the Base OS Management Pack. But considering the situation, additional management packs are also needed:

- An Active Directory integrated DNS server needs the AD Management Pack
- Clustered DNS servers need the Clustered Management Pack

Additionally, if you're monitoring Windows 2000 DNS servers with MOM, the Windows 2000 DNS WMI Provider must be installed. The DNS WMI Provider is available in the Windows 2000 Server Resource Kit, or you can hunt for the DNS WMI Provider using your favorite search engine.

Managing DHCP

Most networks don't use static IP addressing for the desktop environment. So to be able to assign IP addresses, you need to set up a DHCP (Dynamic Host

Configuration Protocol) server. This server has a "pool" of available IP addresses and hands them out one by one if a system asks for it.

This service is very important and needs to be running. If the service stops handing out IP addresses (say, if the pool of IP addresses is empty), it's possible it will stay undetected until users start noticing.

This can easily be solved by installing the Windows Dynamic Host Configuration Protocol Services Management Pack. This pack takes over the monitoring burden. When imported into MOM, it monitors the health of the DHCP server, the availability of IP addresses in the IP pool, and the possibility of rough DHCP servers in the network.

No additional configuration is needed. It automatically detects the servers running DHCP on the network.

Managing WINS

Windows Internet Name Service (WINS) is the old-style network name resolver (NetBIOS) that's mainly used by the Windows 9*x* and NT 4.0 type systems. These systems are not DNS-aware, unlike the windows 200*x* and XP systems. To be able to communicate with other systems on the network, it may use DNS, but it will first try to find the system using NetBIOS. This NetBIOS call can be addressed to a server running the WINS service.

To monitor the availability of the WINS services on the server, you can import the Windows Internet Name Service Management Pack. This management pack alerts you in case the following critical conditions arise:

- WINS is not available.
- The WINS database is corrupt or missing.
- There are errors in the WINS database backup.
- WINS database has reached its limit, indicating availability concerns.
- There are errors in the replication process.

A total of more than 140 rules are defined that monitor the eventlog for issues in the WINS infrastructure, just for Windows 200*x* alone.

Managing RRAS

The RRAS service provides a server or user with connectivity when using a dial-up or VPN connection. This can be used in a situation where a server connects occasionally to the branch office to replicate AD information. However, it's also possible

that the server may be enabled to service VPN connections. If you would like to monitor this in MOM 2005, two versions of this management pack are available:

- Windows Routing and Remote Access Service (RRAS) 2000
- Windows Routing and Remote Access Service (RRAS) 2003

Both versions are supported in MOM 2005 and can be imported if needed. When you import the RRAS 2003 Management Pack, you're able to monitor the RRAS server on the following issues:

- Automatic notification of events indicating service outages
- Performance degradation
- Health monitoring
- Centralized management

This is done by monitoring the following functions that RRAS might need to function correctly:

- The DHCP Relay Agent (IPBOOTP), which makes it possible to receive an IP address from a server behind the RRAS server
- Internet Group Management Protocol (IGMP) Version 2, a router and proxy that makes it possible to transmit and receive (used for streaming media)
- The Multicast Group Manager (MGM), which is used to coordinate more than one multicast protocol
- The Network Address Translation (NAT) protocol, which is used to show only one single IP address on the outside of the network when browsing
- The RIP Version 2 for Internet protocol, which is used to build the routing tables to enable RRAS to route the network packages to the right networks

These are the most elementary functions that the RRAS needs to function correctly.

Also, after importing the management pack, you don't need to configure anything.

Managing DFS

DFS (Distributed File System) can be used to combine several shares on different servers into one location for easier user access. This will also ensure redundancy and less support calls.

Microsoft published a management pack for DFS in the Windows File Replication Services Management Pack. This management pack monitors the following basic functionalities about the DFS environment in your network:

- DFS share availability from a client's perspective: Is it possible to get to the share?
- DFS root, link, and target availability: Is the DFS functioning correctly?
- DFS service health: Are the essential services running?

If you import this management pack, you need to configure client-side monitoring. This is used to verify the users' ability to access the DFS shares supplied on your network. By enabling this, you let MOM act as an end-user that tries to access the DFS share. If it fails, it will fire an alert.

To configure client-side monitoring, perform the following steps:

1. Add the computers you want monitored into the Microsoft Windows Distributed File System Client Side Monitoring computer group.
2. Go to the rule on DFS paths that you want to test for availability. This script parameter can be found in the directory *Management Packs\Rules\Microsoft Windows Distributed File Systems\Windows (All Versions)\Microsoft Windows DFS Client Side Monitoring\Event Rules*.
3. Double-click the **rule** to open the properties window, and then choose the **Response** tab.
4. Select the **script** and click **Edit**.
5. In the **Script Parameters** section, select the parameter **UNCPaths** and then click **Edit Parameter**.
6. In the Value text box, type the DFS shares that need to be tested, with each one *separated by a colon* (for example, \\fileserver1\share**:**\\ fileserver2\share).

Managing Print Servers

This section should prove very handy to you.

How many telephone calls have you received, with the following question: "The printer is not printing. Is it broken?" Every time this occurs, you need to connect to the printer, print a test print, and verify if it's running. The Windows Printing services management pack does this for you.

If you import the management pack, you're able to monitor the health of the print services on the servers and will receive an alert if the server has trouble

printing. No further configuration is needed. This is a quick solution. If a user calls to report the printing trouble, you can tell them that you're not on it, but at it.

Managing Active Directory Services

One of the main pillars of the current enterprise networks is a Directory Service. In a Windows network, in most cases, this is Microsoft Active Directory. If this service isn't running accordingly, people will find your desk pretty quick. Using Microsoft Operations Manager 2005, you're able to monitor its behavior. This includes, but is not limited to, things like Active Directory health, availability, and performance data.

In this section, we'll describe the effort needed to deploy the Microsoft Active Directory Management Pack. This pack will give you a right set of monitoring options, but, due to the important role in the network, it can cause a lot of false alerts.

Shortcuts…

The Latest Version of Management Packs

So now you have a fine state-of-the-art monitoring system to check if everything is okay. But who's going to monitor the monitoring solution. This is done by the MOM Management Pack. Once in a while, however, Microsoft produces major updates on management packs and publishes them. This would mean that you'll need to go and check the Microsoft management pack site for other versions.

But this is where the MPNotifier Management Pack comes in. This management pack monitors the Microsoft Web site and sends a warning event if there's an update on one of the following management packs:

- Microsoft Baseline Security Analyzer
- Exchange 2000
- Exchange 2003
- Operations Manager 2005
- Operations Manager 2000
- Microsoft Systems Management Server (SMS) 2003
- Microsoft SQL Server
- Microsoft Windows Active Directory
- Microsoft Windows Servers Base Operating System
- Microsoft Windows DNS Server

Continued

- Microsoft Windows Internet Information Services
- Microsoft Windows Server Clusters
- Microsoft Exchange Server Best Practices Analyzer Tool
- Microsoft Operations Manager 2005 Web Sites and Services MP
- Microsoft Operations Manager MPNotifier
- Microsoft Virtual Server
- Microsoft Windows Desktop Base Operating System
- Microsoft Windows DHCP Server
- Microsoft Windows Distributed File Systems
- Microsoft Windows File Replication Service
- Microsoft Windows Terminal Services
- Microsoft Application Center
- Microsoft Windows Print Server
- Microsoft Windows Server 2003 Performance Advisor
- Microsoft System Center Data Protection Manager (DPM)

If the versions on the Web site have a higher version than those installed on the system, you will be notified.

Overview of the Active Directory Management Pack

The Active Directory Management Pack (ADMP) is not your ordinary management pack. In my job as a consultant, this is definitely one of the management packs I would chose to demo if a customer wants to know about MOM and its features. It is able to do so much more than Active Directory monitoring on a service level. If you deploy the ADMP in your network, you'll be able to get overviews of all critical processes, check up on replications, detect outages, and so on.

Importing the Active Directory Management Pack requires you to have a number of packs in place. One of which is the MOM Management Pack. Without this pack, MOM will not function correctly, so be sure to use the newest version available on the Microsoft Web site.

The other required packs are the DNS Management Pack and the Windows Base Operating System Management Pack.

Active Directory Management Views

Using the Active Directory Management Pack will give you a lot of views. Each has its purpose: some offer quick access to the CPU performance on a specified domain controller, whereas others are better suited for troubleshooting. There are numerous views, so rather than trying to address them all, we'll briefly address those views that are the most important (in our opinion).

Performance Views

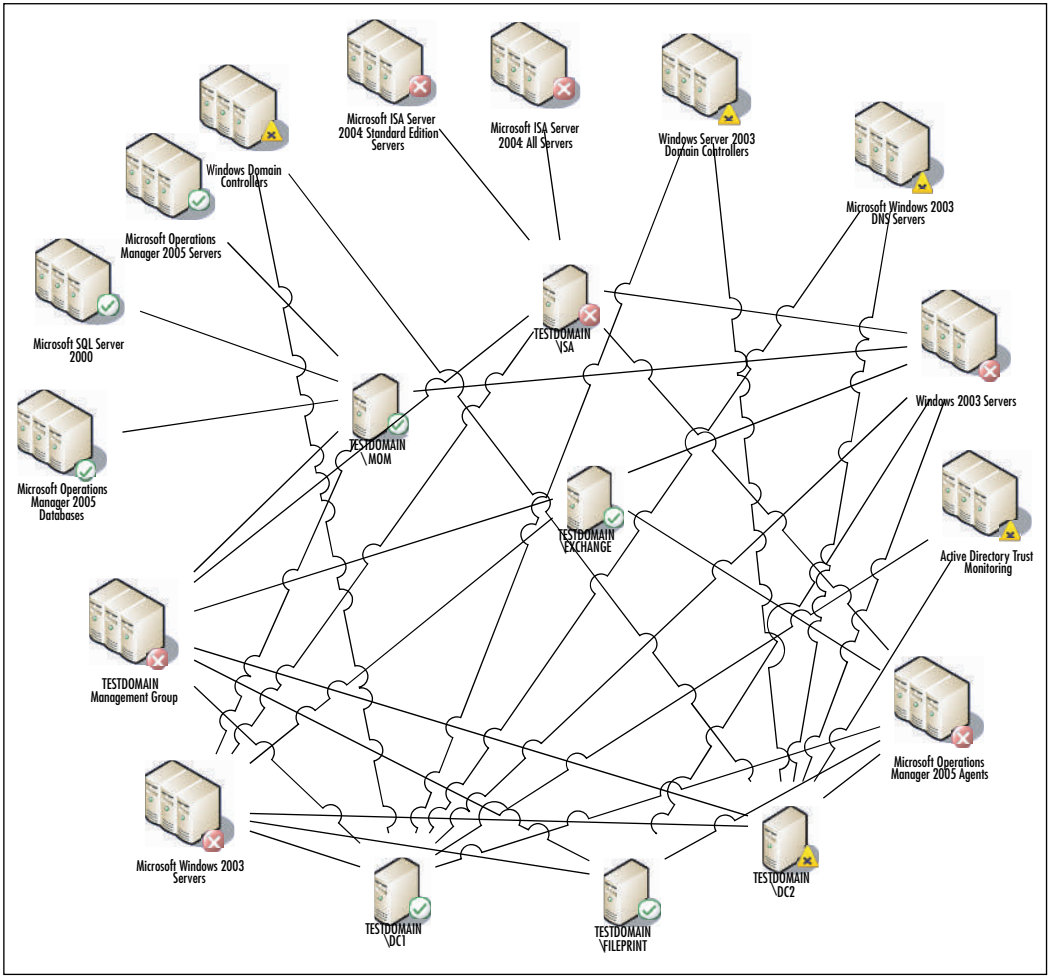
Performance views provide you with easy access to the performance data of the monitored server. If you install the AD Management Pack, you're able to monitor the performance on several counters. These views enable you to troubleshoot several common problems on a major network.

- Discovery\Number of Client Sessions
- Health Monitoring\Active Directory Database
- Health Monitoring\Active Directory DIT/Log Drive Space
- Health Monitoring\Active Directory Log Files
- Health Monitoring\CPU Usage on Active Directory Domain Controllers
- Health Monitoring\Domain Controller Response Time
- Health Monitoring\Global Catalog Response Time
- Health Monitoring\LSASS CPU Usage on Active Directory Domain Controllers
- Health Monitoring\Memory Use on Active Directory Domain Controllers
- Health Monitoring\Processor Queue Length
- Health Monitoring\Role Master Response Time
- Replication Monitoring\Intersite (Compressed) Replication Traffic
- Replication Monitoring\Replication Latency
- Replication Monitoring\Replication Traffic—Inbound Bytes per Second
- Replication Monitoring\Replication Traffic—Outbound Bytes per Second

Diagram Views

Another great feature from the Active Directory Management Pack is the Diagram views. These let you generate a Visio-format view of your domain and site links (see Figure 8.1).

Figure 8.1 Example of a Diagram View



No need to draw a map anymore. MOM is the tool to use in this case. The generated drawing is exportable to Visio, and all the server icons give the status of the particular server, according to the state view. By double-clicking each, you go directly to the event causing the problem—a nice feature.

The following diagram views will be available to you when you import this management pack:

- Replication topology\site links
- Replication topology\connection objects
- Replication topology\broken connection objects

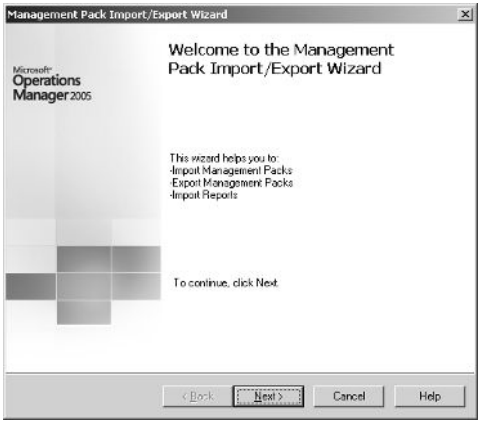
Importing the Active Directory Management Pack

As mentioned earlier, importing the management pack is done after importing the Base Server OS and DNS Management Pack. These are essential to the AD Management Pack deployment. Furthermore, the Active Directory Management Pack is one of the few packs that need to be manually configured before it can function properly.

To import the AD Management Pack, perform the following steps:

1. In the **Navigation** pane, click **Management Packs**.
2. In the **Detail** pane, click **Import/Export Management Packs** to open the **Management Pack Import/Export Wizard**. (See Figure 8.2.)
3. Follow the instructions in the Management Pack Import/Export Wizard and then click **Next** to start the import operation.
4. Select **Import Management Packs and/or Reports**. (See Figure 8.3.)

Figure 8.2 Welcome to the Management Pack Import/Export Wizard



5. Select the location to save the file to, and then click the **Import Management Packs only** button. (See Figure 8.4.)

Figure 8.3 The Import or Export Management Packs Screen

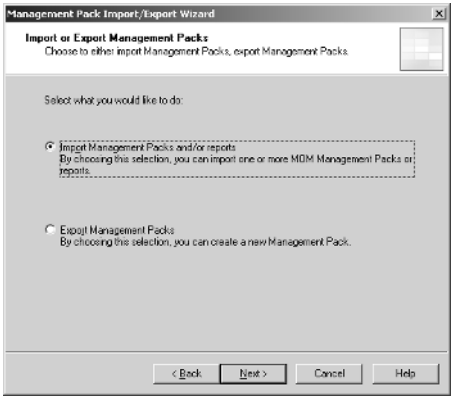
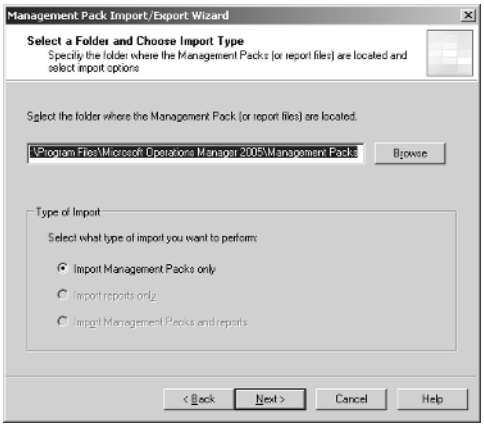


Figure 8.4 Select a Folder Where the Management Pack Is Located



6. Click **Next** to open the **Select Management Packs** screen.
7. Select each management pack to import, and choose the Update Existing Management Pack option. (See Figure 8.5.)
8. Review the selections, and click **Finish** to start the import operation. (See Figure 8.6.)
9. Right-click the **Management Packs** folder on the MOM Administrator console, and then select **Commit Configuration Change**.

Figure 8.5 The Select Management Packs Screen

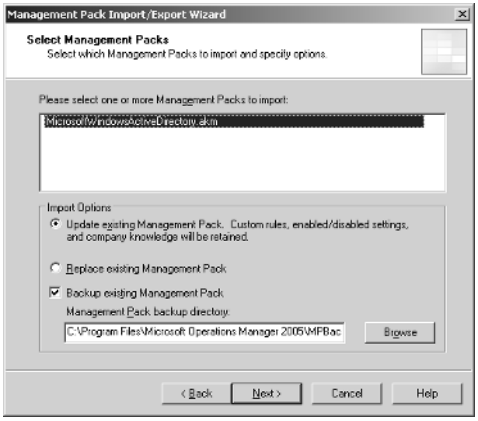
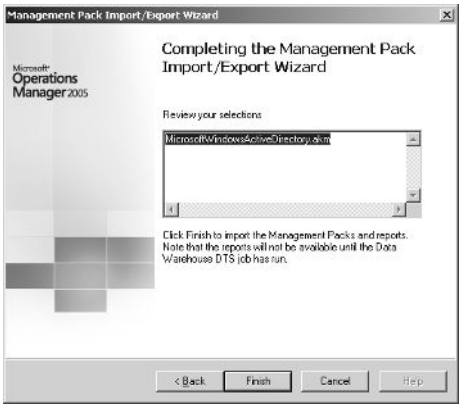


Figure 8.6 Completing the Management Pack Import/Export Wizard



Configuring the Active Directory Management Pack

As we stated earlier, the AD Management Pack needs some configuration settings after being imported. These are not hard to do, and only need to be set once.

Setting the Intersite Replication Latency Threshold

The "intersite replication threshold" is the threshold time for the replication to complete in the entire AD forest. If the replication of the objects is greater than the threshold value, MOM will fire off an alert that the replication is being done slowly.

To set the intersite replication threshold value, perform the following steps:

1. In the MOM 2005 Administrator console, double-click **Management Packs**, double-click **Rule Groups**, double-click **Microsoft Windows**

Active Directory (enabled), double-click Active **Directory Windows 2000 and Windows Server 2003 (enabled)**, and then double-click **Active Directory Availability (enabled)**.

2. Click **Event Rules**.
3. In the right pane, double-click **Script - AD Replication Monitoring**.
4. On the **Responses** tab, click the script named **AD Replication Monitoring**, and then click **Edit**.
5. Under Script parameters, double-click **IntersiteExpectedMaxLatency**.
6. In Value, type the value (in minutes) for the maximum expected replication latency between domain controllers.
7. Click **OK** three times.

Specifying Domain Controllers for Replication Latency Data Collection

1. In the MOM 2005 Administrator console, double-click **Management Packs**, and then double-click **Computer Groups**.
2. In the right pane, right-click **Active Directory Replication Latency Data Collection - Sources**, and then click **Properties**.
3. On the **Included Computers** tab, select the domain controllers that you want to track replication latency data from, and then click **OK**.
4. Right-click **Active Directory Replication Latency Data Collection - Targets**, and then click **Properties**.
5. On the **Included Computers** tab, select the domain controllers that you want to track replication latency data to, and then click **OK**.
6. In the left pane, right-click **Management Packs**, and then click **Commit Configuration Change**.

Monitoring Active Directory

As Active Directory is one of the most important parts of your network, you need to take great care to let it run perfectly. If you don't want your MOM operator console open all the time, there's a little tool you can use called Operator Console Notifier, which is available in the resource kit of MOM.

Be sure to check every alert coming from this pack. One of the most important things to remember is to resolve the problem, not to simply fix the symptoms.

If a problem is reported to MOM, research the trouble in order to find the best solution. That way, the problem will not come back, and your MOM will be more accurate.

To give an indication on the power of MOM, Microsoft uses MOM 2005 on the corpnet. This is all monitored by MOM and all problems regarding AD are addressed automatically.

Generating Active Directory Reports

The AD Management Pack comes with a rich set of reports. For those who already have a MOM reporting server, you'll love this. If you don't have a MOM reporting server, you'll find this is one of MOM's great features, giving you much more information than four days in a default MOM environment.

There are a few interesting reports you can review on a weekly base:

- AD Domain Changes
- DC Disk Space
- The AD Replication Latency Report
- AD SAM Account Errors

In addition to the preceding reports, a number of reports should be reviewed monthly, such as:

- Active Directory Reports
  - The DC Replication Bandwidth
  - AD Machine Account Authentication Failures
  - AD Domain Controllers
- Operational Health Analysis Reports
  - The Most Common Alerts by Rule Group
  - The Most Common Events by Computer

Agentless Monitoring

The Active Directory Management Pack does not support agentless monitoring.

Managing Group Policy

In every Windows 2000 and later network, group policies (GPO) are enrolled, even if you haven't set any. By default, there are two GPOs: the Default Domain Controller Policy and the Default Domain Policy. These make valuable changes to servers and systems in the network and can involve all types of settings, such as security, software deployment, and user environment. This is why the processing of group policies might be monitored.

Best Practices According to Microsoft

The Group Policy Management Pack is not supported on any servers before Windows 2003, or any desktop operating system.

An Overview of the Group Policy Management Pack

The Group Policy Management Pack monitors and responds to the various health states of the delivery and application of the Group Policy Object (GPO). The focus of the management pack is the Windows 2003 Server operating system and is not intended to be used on the desktop operating system.

Group Policy Management Pack Components

The Group Policy Management Pack is based on a few objects; the management pack does not contain any scripts of attributes. It encapsulates a few rules that monitor several GPO events as they are logged into the application eventlog. No other objects are created after importing the management pack.

The following rules are imported with the management pack:

- Microsoft Windows Group Policy\Group Policy Client Side Extension Processing\Group Policy - Disk Quota
- Microsoft Windows Group Policy\Group Policy Client Side Extension Processing\Group Policy - Folder Redirection
- Microsoft Windows Group Policy\Group Policy Client Side Extension Processing\Group Policy - Registry
- Microsoft Windows Group Policy\Group Policy Client Side Extension Processing\Group Policy - Scripts

- Microsoft Windows Group Policy\Group Policy Client Side Extension Processing\Group Policy - Security
- Microsoft Windows Group Policy\Group Policy Client Side Extension Processing\Group Policy - Software Installation
- Microsoft Windows Group Policy\Group Policy Machine and User Processing

Importing the Group Policy Management Pack

The management pack is imported the same way as other management packs, but you do need to edit the MOM configuration after importing it.

If you use the Active Directory Management Pack along with the Group Policy Management Pack, disable the *Active Directory – UserEnv* Processing Rule Group; otherwise, both will fire when issues arise.

This can be done by performing the following actions:

1. In the administrator console, choose Management Pack\Rule groups\Microsoft Windows Active Directory (enabled)\Active Directory Windows 2000 and Windows Server 2003 (enabled), then right-click Active Directory – UserEnv, and select Properties.
2. Uncheck the Enabled check box.

Monitoring Group Policy

The Group Policy Management Pack is an event-based monitor. It does not do any scripting to provide extra information. The management pack will continually check the following functions:

- Group policy core infrastructure/registry client-side extension
- Scripts client-side extension
- Software Installation client-side extension
- Security client-side extension
- Folder redirection client-side extension
- Disk quota

Using the Group Policy Knowledge Base

One of the nice things about the Group Policy Management Packs is the knowledge base included in the pack. This is essential when troubleshooting a serious problem.

For example, in the GPO Management Pack, there's a rule called Machine Required Resources Not Available. This rule has specific information on how to resolve the error you're encountering.

Verbose logging can assist in debugging this error. Refer to KB Q221833—How to Enable User Environment Debug Logging in Retail Builds of Windows to enable userenv logging. The log file will detail the specific error. If none of the preceding actions identified the problem, follow the additional steps given in the "Troubleshooting Group Policy" white paper.

This makes the troubleshooting of GPO-related problems a lot easier, as you can see. There is a piece of knowledge about troubleshooting GPOs built into the management pack.

Summary

In this chapter we took a look at the AD Management Pack, which requires almost no configuration. Importing this management pack will give you information like replication, AD health, and so on. However, AD is not the only network service in operation. Many network services are waiting to be monitored, such as DNS, DHCP, and DFS. Last topic of interest was the use of the Group Policy Management Pack. This management pack is intended to monitor the GPO processing on the servers (not the desktops).

Solutions Fast Track

Managing Network Services

- ☑ Before importing the DNS Management Pack, review the MP guide. This will give you insight on how to set up your DNS monitoring environment.
- ☑ If you run a Windows 2000 server DNS, you need to install the Windows 2000 DNS WMI provider on that server. Without it, the DNS Management Pack will not function correctly.
- ☑ The DHCP management pack will configure automatically.
- ☑ The WINS management pack will configure automatically.
- ☑ The RRAS management pack is available in two versions: the Windows 2000 and 2003 versions. After importing the correct version, there's no need to configure anything.

- ☑ After importing the DFS Management Pack, you need to configure "Client Side Monitoring" by setting the monitored shares as parameters in the script.
- ☑ The print services management pack is a quick win. After importing the management pack, you're able to receive information on the printer status of the print services. After importing the management pack, there's no need to configure it since it's done automatically.

Managing Active Directory Services

- ☑ Import the Active Directory Management Pack after importing the DNS Management Pack.
- ☑ After importing the management pack, you must configure it.
- ☑ You must wait 24 hours for the initial triage.
- ☑ Issues may arise in which the ADhelper Object has trouble running scripts. See Chapter 13.

Managing Group Policy

- ☑ The Group Policy Management Pack is used to monitor the GPOs that are processing on the servers.
- ☑ The GPO Management Pack only forwards events; it does no resolving.
- ☑ The GPO Management Pack is mostly used to troubleshoot policy issues.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: I have a network that's running multiple domain controllers. We imported the AD Management Pack, but there seem to be a lot of domain controllers that aren't able to finish scripts. Each time I get an Unknown Object message in the event.

A: This happens because the ADMP uses a lot of calls to the IOOMADsInfo. This object is used to connect to the AD. If the script calls it on a server that does not have this class installed, the script will fail and the MOM server will generate an error.

Q: Is it possible to run the AD Management Pack without the DNS MP?

A: Microsoft best practices say it shouldn't be done. This doesn't mean it won't run, however. If Microsoft proclaims it should be imported in conjunction with the DNS MP though, you should do so.

Q: Do I really need to monitor all these network services? They never seem to fail.

A: It's not a must, but if your MOM server can handle the load and the license, why not? Even though it hasn't failed, you should think of it with the perspective that "It has not failed yet." Plus, it's easy to deploy and will save you time when one or more services do fail.

Q: I want to monitor the desktops in my network for GPO processing troubles. Can I do this?

A: Well, there *is* a GPO Management Pack, but it's only intended for the server.

Q: I have Windows 2000 DNS server. Do I need to manually install the WMS DNS provider on every DNS server?

A: Yes, you need to install the DNS provider on every server. If you use the file transfer server, this can be done automatically. You should also be able to write a response script on the DNS event. This script should download, and installs the DNS provider automatically.

Chapter 9

Managing Intel-Based Hardware

Solutions in this chapter:

- **Managing Server Hardware**
- **Managing Intel-Based HP Servers**
- **Managing Dell Servers**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

So by now we've got it all worked out. The MOM system is monitoring the Microsoft environment, and everything is running smoothly. There are still a couple of weak points, however. For instance, how can we tell if all the disks in the RAID controller or the memory are okay? Unless you put in the extra effort, MOM won't be able to determine this. It's at these times when hardware monitoring comes in handy.

Managing Server Hardware

The main problem of hardware monitoring is hardware support. The hardware should be able to report to Windows, or even better, to the event log for easy access to hardware events. Another option is to use Windows Management Instrumentation (WMI), but that's a bumpy road. You need to know how to set up the appropriate rules and providers, and you need to have a WMI provider that's able to support hardware queries. In short, this is not the way you should go unless there's no other option.

If you scan the MOM Management Pack site at Microsoft, you'll notice a couple of hardware manufacturers that supply their own management packs. They can provide essential information about the hardware of the server out of the box. That means no WMI or other hardware configuration; just follow the deployment guide, and you are off monitoring the hardware.

If you can influence your organization's hardware-buying decisions, you should recommend buying hardware from one of the aforementioned manufacturers because using this hardware will be a time-saver. If your organization can afford the investment, check if these manufacturers' new servers come with a Windows hardware monitor. This, in conjunction with the MP wizard from the resource kit, can make miracles happen.

Best Practices According to Microsoft

Microsoft advises that you use hardware from the Windows Server catalog at www.microsoft.com/windows/catalog/server/. This site offers complete information on systems built for the Windows Server 2003 family. Catalogs for other Microsoft operating systems are also available. See www.microsoft.com/whdc/hcl/default.mspx.

Some Independent Advice

If you're going to buy some new servers to deploy the MOM infrastructure, be sure to check the Microsoft MOM management packs Web site (www.microsoft.com/management/mma/catalog.aspx) to see if there's a management pack for the brand and type of server you're about to buy. If not, you might do well to think twice. There are many reasons to select a vendor that has a management pack posted on the Microsoft site. One of them is the possibility to be proactive in case of an error on the hardware level. I once imported the Dell management pack at a customer location. This network had over 200 servers in it and we found over six servers that had hardware errors on them, including RAID controllers that were running one disk short. If MOM didn't detect them, they would have run until the second disk failed, leading to a restore action, and a fair amount of time loss. This is one of the points you can make to yourself or your manager. It can save you a lot of problems if you buy a MOM-supported piece of hardware.

Shortcuts…

Vendor-Supplied Software

You know the drill: new server, install OS, install application, test, deploy. Yet so often I still find myself in companies that don't install the vendor-supplied software on the server boxes. This happens for various reasons. But do yourself a favor: install that piece of software. If you're going to use a monitoring solution in your network, you probably need it anyway. With the low prices of today's disk space, that shouldn't be a problem anymore.

An Overview of Hardware Management

As we said, hardware can be monitored by MOM using vendor-supplied management packs. However, another layer also needs to be monitored—the layer known as the OS or operating system.

To monitor the operating system, you must import a separate management pack. This management pack monitors the events on a Windows 2000 or Windows Server

2003 system in the application and system eventlog. If these events occur, the information in the management pack will lead you to the solution of the problem.

Hardware Management Best Practices

If you're going to do hardware monitoring on the server, be sure to import the hardware management pack after the Windows Base OS management pack is running smoothly. This way you're sure that the messages you're receiving are not caused by the Windows base OS management pack.

It is not always supported to monitor the hardware from the MOM console. The server might not be able to support the load or the hardware has no management pack available. In such cases, there are other options available to provide hardware support, such as using a new server and deploying Microsoft Virtual server 2005. This, together with the Virtual Server Migration Toolkit (part of the Microsoft Automated Deployment Services feature pack), virtualizes the non-supported hardware to the new server running on supported hardware. This way, there's a form of hardware support on the services. Of course the cost may at first seem a major drawback in this scenario, but hang on—there are some pros to this also. MOM uses a physical device license model, which means you need to have a license for the host server only. After virtualizing five servers, the savings can amount to as much as $1600 (at the time of this writing)—and this is in addition to the better response support and durability. Your manager may be much more willing to consider it after hearing this.

If you're unable to arrange any of these options, there might be another way to do hardware monitoring—by creating a notification rule that fires every day and notifies the operator to check, say, a particular disk array. This way, each day you're given a reminder to walk past the server(s).

Managing Base OS Functions

The Base OS Management Pack is available in two flavors: the server operating system variety and the one for the desktop operating system. In this chapter, we'll address the availability and other aspects of the desktop management pack, but it won't be our main focus. Instead, we'll concentrate on the Base Server OS Management Pack.

An Overview of the Base OS Management Packs

The Base Server OS Management Pack is used to monitor performance and events on the OS level. Importing this into your MOM infrastructure will give you an instant knowledge and view of the operating system below the surface. By doing this, you'll be able to monitor memory and processor usage depending on the MOM infrastructure configuration up to a year earlier.

Server Operating Systems

The Base Server OS Management Pack monitors your entire system without you having to open Performance Monitor or any of the available consoles, such as Event Viewer.

It will monitor the state of the network connections, services, processors, and memory allocation. The Base Server OS Management Pack won't monitor usage of the MOM service. This is done through the MOM Management Pack. Everything else is done by way of the Base Server OS Management Pack.

The management pack has a lot of intelligence in it, so it will act based upon the hardware configuration on the server. It will support the full monitoring functionality on agent-managed servers. As for this requirement, the agentless monitoring of Windows NT 4.0 enjoys only limited support (see Table 9.1).

Table 9.1 Server Operating System Support in the Windows-Based Server OS Management Pack

			Support on	
Scenario	**Description**	**NT 4.0**	**2000 Server**	**Server 2003**
Service and application management	Core Windows service up/down status Unexpected service terminations Service configuration issues Service account and authentication issues	Core Windows service up/down status only	YES	YES
Reliability	Detects recurring application terminations Gathers data on system shutdowns (for shutdown reporting) Reports system failures (for stop error reporting)		YES	YES
Storage	Shares availability issues Shares configuration issues Local storage resource availability Local storage free space File system integrity and corruption issues	Local storage free space only	YES	YES

Continued

Table 9.1 continued Server Operating System Support in the Windows-Based Server OS Management Pack

		Support on		
Scenario	**Description**	**NT 4.0**	**2000 Server**	**Server 2003**
Networking	IP address conflicts Disconnected network adapters Duplicate network names		YES	YES
Performance measuring	For most commonly used performance data		YES	YES
Performance threshold monitoring	Physical Disk — Avg. Disk sec/ Physical Disk — Avg. Disk sec/Read Memory — Pages/sec Processor — % Processor Processor — % DPC Processor — % Interrupt Time Memory — % Committed bytes in use Memory — Available Megabytes	YES	YES	YES
State monitoring and service discovery	Base OS services Storage Messenger service Computer browser Logical Disk Manager service Dynamic Host Configuration Protocol (DHCP) client Domain Name Service (DNS) client Remote Procedure Call (RPC) health Server service Transmission Control Protocol/Internet Protocol (TCP/IP) NetBIOS Helper service	YES	YES	YES

Continued

Table 9.1 continued Server Operating System Support in the Windows-Based Server OS Management Pack

			Support on	
Scenario	**Description**	**NT 4.0**	**2000 Server**	**Server 2003**
	Hardware discovery Event log Workstation service			

Workstation Operating Systems

Use the Windows Desktop Base OS Management Pack with MOM 2005 to monitor Windows XP Professional. This MP monitors the performance, health, and availability of Windows XP Professional computers.

Importing the Server OS Management Pack

Importing the Base Server OS Management Pack is straightforward. There's little to no configuration needed after the installation of the management pack.

Considering disk free space monitoring, you might decide to edit the default thresholds (see Table 9.2). The thresholds may seem a little low, but in the end they will depend on your own server usage.

Table 9.2 Default Disk Space Threshold Values

Drive	Warning Threshold	Error Threshold
All volumes	N/A	100MB
Non-system drives	500MB and 10% or less free space	250MB and 5% or less free space
System drives	500MB and 10% or less free space	250MB and 5% or less free space

If you have various versions of Windows running on your network, there might be a different demand. For example, the old Windows NT 4.0 box that's running on the network might not have that much disk space left anymore. To prevent warnings about disk space, it's possible to change the default setting on the OS level. Simply go to the Administration console and open **Management packs\Rule groups\Microsoft Windows Base Server Operating system*OS Type*\State moni-**

toring and service discovery\Event rules\Run storage state monitoring. For example, if you want to change the default settings for the Windows NT 4.0 boxes in your network, simply browse to Management packs\Rule groups\Microsoft Windows Base Server Operating system*Windows NT 4.0*\State monitoring and service discovery\Event rules\Run storage state monitoring.

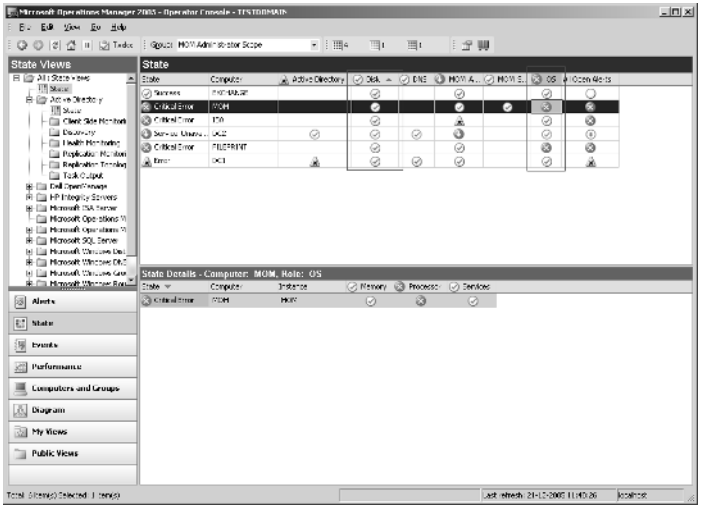
Monitoring Server Operating Systems

If the initial settings are made, you can use the various views the Base Server OS Management Pack offers. Personally, I like the state-view screen of the MOM console because it offers a handy overview.

After importing the management pack, the following information is added to the State view:

- **Disk** If this changes state, just select the yellow or red sign and in your view pane all disks will be shown with the green, yellow, or red sign.
- **OS** If this changes state, just select the yellow or red sign, and in your view pane the items memory, processor, and services will appear. (See Figure 9.1.)

Figure 9.1 The MOM Operator Console in State View



Clicking either of these signs will bring you straight to the alert that caused the problem. As always, the probable solution is hidden under the Product Knowledge and Company Knowledge tab.

If you select the Performance view in the navigation pane, you'll be able to choose the various counters imported by the management pack.

Managing Intel-Based HP Servers

One of the vendors that supplied Microsoft with a management pack for the hardware is Hewlett-Packard. The management pack published supports two types of servers: the HP ProLiant and the HP integrity servers.

NOTE

Remember, it is all in the manufacturer-supplied server software (like Dell OpenManage and HP Insight management). Deploy this software on all servers and the MOM management pack will work directly.

Shortcuts…

When Importing the Management Pack

The Hardware Monitoring Pack is one of the first management packs you need to import. You start with the Base OS, wait for the event storm that comes after the import, resolve the issues from that storm, and install the Hardware Monitoring Pack.

An Overview of Available HP Management Packs

The two management packs for the HP ProLiant and HP Integrity servers are from HP itself. This isn't a problem since every management pack that's published on the Microsoft site must meet several strict rules. One of these rules is the availability of knowledge in the Knowledgebase of the management pack. Of course it would be weird for a hardware vendor to deploy a package to support hardware without displaying and providing the knowledge it has about its product. But let's use the following sections to take a closer look at the two packs.

The Integrity Management Pack

The Integrity Management Pack is the next version of the HP Insight Manager Management Pack. To successfully import the management pack, you need to make sure the Insight Manager Management Pack is completely removed.

After importing the management packs, the following computer groups must be visible in the MOM Operator console (and the Administration console, of course):

- HP Integrity Insight Management Agents
- HP Integrity Servers
- HP Systems Insight Manager Hosts

The following rule groups will be added to the MOM environment:

- HP Integrity Servers
- HP Integrity Servers\HP Insight Management Agents
- HP Integrity Servers\HP Insight Management Agents\Base Hardware
- HP Integrity Servers\HP Insight Management Agents\Cluster Hardware
- HP Integrity Servers\HP Insight Management Agents\Network Interface
- HP Integrity Servers\HP Insight Management Agents\Server Storage
- HP Integrity Servers\HP Insight Management Agents\State Monitoring and Service Discovery
- HP Integrity Servers\Servers

The ProLiant Management Pack

The ProLiant Management Pack is more or less the same since, although it addresses another piece of hardware, it still monitors the HP hardware. They even use the same management pack guide.

The following computer groups should be available after importing:

- HP ProLiant Insight Management Agents
- HP ProLiant Servers
- HP ProLiant Servers BL
- HP ProLiant Servers DL
- HP ProLiant Servers ML
- HP Systems Insight Manager Hosts

The following rule groups should be visible after importing the management pack:

- HP ProLiant Servers
- HP ProLiant Servers\HP Insight Management Agents
- HP ProLiant Servers\HP Insight Management Agents\Base Hardware
- HP ProLiant Servers\HP Insight Management Agents\Cluster Hardware
- HP ProLiant Servers\HP Insight Management Agents\Environmental
- HP ProLiant Servers\HP Insight Management Agents\Network Interface
- HP ProLiant Servers\HP Insight Management Agents\Remote Management Processor
- HP ProLiant Servers\HP Insight Management Agents\Server Storage
- HP ProLiant Servers\HP Insight Management Agents\State Monitoring and Service Discovery
- HP ProLiant Servers\Servers

The Insight Manager Management Pack

The Insight Manager Management Pack cannot be installed on a MOM 2005 server. But there's no need to do so because the Integrity and ProLiant Management Pack supersedes this one. The best practice recommendation from Microsoft is to use the most current management pack available. As this one is replaced by two, it is obsolete.

Uninstalling the Insight Management Pack for MOM 2000

To uninstall the Insight Management Pack for MOM 2000, perform the following steps:

1. Access the **MOM 2005 Operator console** and verify that no pending alerts are displayed. Resolve any pending alert listed in the MOM 2005 Operator console before proceeding to step 2.
2. Exit the **MOM 2005 Operator console**, and start the **MOM 2005 Administrator console**.
3. Right-click each HP IMP subfolder under **Computer Groups**, and select **Delete Computer Group**. Delete all of the following computer groups:
   - Computer Groups\HP Insight Management Agent Version 4.60
   - Computer Groups\HP Insight Management Agent Version 4.70

- Computer Groups\HP Insight Management Agent Version 4.80
- Computer Groups\HP Insight Management Agent Version 4.90
- Computer Groups\HP Insight Management Agent Version 5.00
- Computer Groups\HP Insight Management Agent Version 5.10
- Computer Groups\HP Insight Management Agent Version 5.20
- Computer Groups\HP Insight Management Agent Version 5.30
- Computer Groups\HP Insight Management Agent Version 5.40
- Computer Groups\HP Insight Management Agent Version 5.50
- Computer Groups\HP Insight Management Agent Version 6.0
- Computer Groups\HP Insight Management Agent Version 6.10
- Computer Groups\HP Insight Management Agent Version 6.20
- Computer Groups\HP Insight Management Agent Version 6.30
- Computer Groups\HP Insight Management Agent Version 6.40
- Computer Groups\HP Insight Management Agent Version 7.10
- Computer Groups\HP Insight Management Agent Versions–All
- Computer Groups\HP Insight Management Agent Versions newer than 6.40
- Computer Groups\HP Insight Management Agent Versions newer than 7.10
- Computer Groups\HP Insight Manager 7 Server
- Computer Groups\HP Remote Insight Host System
- Computer Groups\HP Systems Insight Manager System

4. Select the **Computer Attributes** folder.
5. Right-click each HP Insight computer attribute, and then select **Delete**.
   - Computer Attributes\HP Insight Management Agent Installed
   - Computer Attributes\HP Insight Management Agent Version Number
   - Computer Attributes\HP Insight Manager 7
   - Computer Attributes\HP Remote Insight
   - Computer Attributes\HP Systems Insight Manager

6. Right-click the top-level HP IMP **Rule Groups** folder, and then select **Delete**.
7. Select **Delete the Rule Group and All Child Rule Groups**. (See Figure 9.2.)

Figure 9.2 The Delete Rule Group Dialog

8. If an error message displays, proceed with step 9 to disable the remaining rule groups. If no error message displays, proceed to step 10.
9. Right-click the remaining HP IMP Rule Groups, select **Properties**, and deselect the **Enabled** check box to disable the rule groups. No further processing will occur under these rule groups.
10. Right-click each HP IMP item in the **Scripts** folder, and then select **Delete**.
    - Scripts\Compaq::CompaqURLScript
    - Scripts\HP::HPIM7URLScript
11. Right-click each HP IMP item under the Providers folder, and then select **Delete**.
    - Providers\Compaq::Process-Handle Count-cpqnimgt-15-minutes
    - Providers\Compaq::Process-Handle Count-cpmgstor-15-minutes
    - Providers\Compaq::Process-Private Bytes-cpqnimgt-15-minutes
    - Providers\Compaq::Process-Private Bytes-cpmgstor-15-minutes
12. Open the **MOM 2005 Operator console**.
13. Right-click HP Insight Management under the Public View folder, and select **Delete**.
    - HP Insight Management
    - HP Insight Management\HP Insight Management Agents

- HP Insight Management\HP Insight Management Agents\Device Error Alerts
- HP Insight Management\HP Insight Management Agents\Event Notifier Alerts
- HP Insight Management\HP Insight Management Agents\Foundation Agent Alerts
- HP Insight Management\HP Insight Management Agents\NIC Agents Alerts
- HP Insight Management\HP Insight Management Agents\Remote Monitor Alerts
- HP Insight Management\HP Insight Management Agents\Server Agents Alerts
- HP Insight Management\HP Insight Management Agents\Storage Agents Alerts
- HP Insight Management\HP Insight Management Agents\Web Agent Alerts
- HP Insight Management\HP Insight Management Agents\Discovery
- HP Insight Management\HP Insight Management Agents\Discovery\Insight Management Agent Versions
- HP Insight Management\HP Insight Manager 7
- HP Insight Management\HP Insight Manager 7\Insight Manager Agent 7 Alerts
- HP Insight Management\HP Insight Manager 7\ Discovery
- HP Insight Management\HP Insight Manager 7\Discovery\Insight Manager 7 Servers
- HP Insight Management\HP Remote Lights-Out
- HP Insight Management\HP Remote Lights-Out\Remote Lights-Out Alert
- HP Insight Management\HP Remote Lights-Out\Discovery
- HP Insight Management\HP Remote Lights-Out\Discovery\Remote Insights Host
- HP Insight Management\HP Systems Insight Manager

- HP Insight Management\HP Systems Insight Manager\HP Systems Insight Manager Alerts
- HP Insight Management\HP Systems Insight Manager\Discovery
- HP Insight Management\HP Systems Insight Manager\Discovery\HP System Insights Manager Servers

With these steps completed, the HP ProLiant Management Pack for MOM 2005 can now be installed.

Importing the HP Management Packs

The import of the HP management pack follows the same procedure as the other management packs in this book. However, there are a couple of prerequisites you need to be aware of.

The Integrity Management Pack

Only import the Integrity Management Pack if you intend to monitor Integrity server. Because the management pack will automatically detect types of servers, it will know when you're not using any Integrity server. This will not give any direct problems, but it will fill the database without having a function.

Before you can import the management pack, you need to make sure the receiving configurations are equipped to be monitored by this management pack. The following configuration settings must be set on the system:

- SNMP services must be active on all Integrity servers to be managed before installing the HP Insight Management Agents. SNMP is required locally on each managed HP system for the correct installation and operation of the Insight Management Agents.
- HP Insight Management Agents versions 2.3 to 3.0 must be installed and active on all HP Integrity servers to be managed using MOM 2005 and the HP Integrity Management Pack.

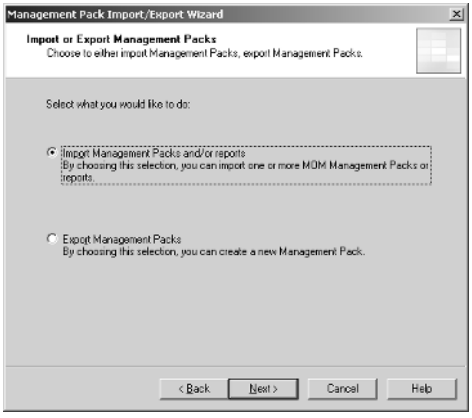
Perform the following steps to import the management pack:

1. In the **Navigation** pane, click **Management Packs**.
2. In the **Detail** pane, click **Import/Export Management Packs** to open the Management Pack Import/Export Wizard. (See Figure 9.3.)

Figure 9.3 The Management Pack Import/Export Wizard Welcome Screen

3. Follow the instructions in the **Management Pack Import/Export Wizard**, and afterward click **Next** to start the import operation.
4. Select **Import Management Packs and/or reports**. (See Figure 9.4.)

Figure 9.4 The Import or Export Management Packs Screen



Select the location to save the file to, and then choose the **Import Management Packs Only** option. (See Figure 9.5.)

7. Click **Next** to launch the **Selection** screen.
8. Select each management pack to import, and then choose **Update** (see Figure 9.6).

Figure 9.5 Selecting a Folder Where the Management Pack Is Located

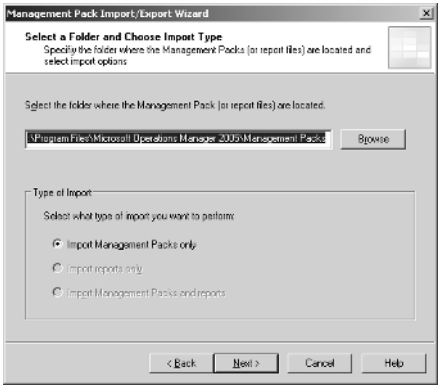
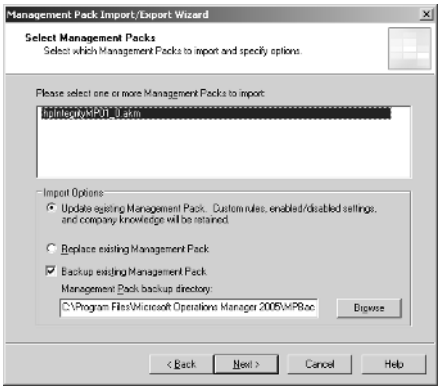


Figure 9.6 The Select Management Packs Screen



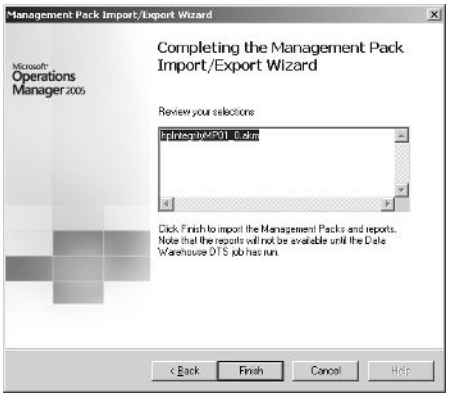
Shortcuts…

What Type of Import to Choose

There's a real need to know what type of import should be used. If you select Update, the management pack will install and add information to the management pack. If you choose Replace, the management pack will be removed and the new one imported. This has a big drawback in that all company information stored in the management pack will be removed. Thus, your best option is to use Update, and if that doesn't work the way you planned, use Replace.

9. Review the selections, and click **Finish** to start the import operation. (See Figure 9.7.)

Figure 9.7 Completing the Management Pack Import/Export Wizard Screen



10. Right-click the **Management Packs** folder on the MOM **Administrator** console, and select **Commit Configuration Change**.

The ProLiant Management Pack

Before installing the ProLiant Management Pack, there are a few prerequisites:

- SNMP services must be active on all HP ProLiant servers to be managed before installing the HP Insight Management Agents. SNMP is required locally on each managed HP system for the correct installation and operation of the Insight Management Agents.
- HP Insight Management Agents versions 5.50 to 7.10 must be installed and active on all HP ProLiant servers to be managed using MOM 2005 and the HP ProLiant Management Pack.

Repeat the same steps as outlined in the section on importing HP Management Packs, "The Integrity Management Pack."

The Insight Manager Management Pack

There's another management pack you can use to monitor the HP server: the HP Insight Manager Management Pack. At the time of this writing, this management pack was listed as supporting MOM 2005. However, when going trough the readme, HP states it can not import this management pack into MOM 2005.

Configuring and Using the HP Management Packs

There's no configuration involved besides the HP Insight Manager and the SNMP. After importing the results from the discovery, scripts will return. This may take a while depending on the attribute discovery cycle in the MOM infrastructure. To speed up the process, go to Administration\Agent Managed Computers. Once there, select the system that needs to be monitored, right-click it and choose **Run Attribute Discovery Now**.

The Integrity Management Pack

As described in the previous sections, importing the management pack is the first step towards monitoring the hardware. But how to monitor it all? And more specifically: How to monitor it all using the Integrity Management Pack?

The HP management packs for Integrity servers includes tasks to provide easy access to several areas of operational management.

The HP System Management Home Page

Selecting the HP System Management task will open the system management home page on the server. Keep in mind that this page is opened on port 2381 using the following command line operation, **https://$TargetComputer$:2381/**, since this is not a common port and you might need to open up the firewall.

To launch the HP System Management home page task:

1. Open the **MOM Operator console**.
2. Select **Public View**.
3. Select a computer from the **Computers** view under the **HP ProLiant Servers** folder or the **HP Integrity Servers** folder.
4. Select the **Tasks** button on the menu bar to display the **Tasks** pane.
5. In the **Tasks** pane, expand the HP Integrity Servers folder.
6. Select **HP System Management Homepage**. A new browser window opens.
7. Log in to the **HP System Management Homepage**.

HP Systems Insight Manager

HP Systems Insight Manager is used to do life-cycle management for systems on the domain/network. HP did a good job creating this task—if there are any issues,

MOM will notice it first and you'll be able to quickly log the hardware error into the database.

To launch the HP Systems Insight Manager task, perform the following steps:

1. Open the **MOM Operator console**.
2. Select **Public View**.
3. Select a computer from the **Computers** view under the **HP ProLiant Servers** folder or the **HP Integrity Servers** folder.
4. Click the **Tasks** button on the menu bar to display the **Tasks** pane.
5. In the **Tasks** pane, expand the **HP ProLiant Servers** folder or the **HP Integrity Servers** folder.
6. Select the **HP Systems Insight Manager**. A new browser window opens.
7. Log in to the **HP Systems Insight Manager**.

The HP Management Processor Task

The HP Management Processor task is only available if the HP Integrity servers are deployed on the network. Using this task will open a Web interface on the server that enables you to perform hardware security and maintenance online. This task has the same function as the ProLiant task HP Lights-Out Management Processor.

To launch the HP Management Processor task, perform the following steps:

1. Open the **MOM Operator console**.
2. Select **Public View**.
3. Select a computer from the **Computers** view under the **HP Integrity Servers** folder.
4. Click the **Tasks** button on the menu bar to display the **Tasks** pane.
5. In the **Tasks** pane, expand the **HP Integrity Servers** folder.
6. Select **HP Management Processor**. The **Launch Task Wizard** opens.
7. Click **Next**.
8. Click **Next** when prompted to edit the command-line task parameters. The default command-line entry should not require editing.
9. Verify the computer listed in the **Targets** pane is the correct server, and then click **Next**.
10. Click **Finish**.

11. Select **Task Status** under the **HP Integrity Servers** folder from **Public View**.
12. Locate and select the task launched.
13. Select the **Properties** tab on the **Event Details** pane.
14. Select the hyperlink to open a browser interface to the HP Management Processor on the associated HP Integrity server.

The ProLiant Management Pack

The ProLiant Management Pack has a lot of similarities with the Integrity Management Pack. There are also two different tasks in the management pack. These two—HP Lights-Out Management Processor and Computer Model Discovery—provide HP/Compaq-specific functionality.

The HP System Management Home Page

Selecting HP System Management task will open the system management home page on the server. Keep in mind that this page is opened on port 2381 using the following command line, **https://$TargetComputer$:2381/**, since this isn't a common port and you may need to open the firewall.

To launch the HP System Management home page task, do the following:

1. Open the **MOM Operator console**.
2. Select **Public View**.
3. Select a computer from the **Computers** view under the **HP ProLiant Servers** folder or the **HP Integrity Servers** folder.
4. Select the **Tasks** button on the menu bar to display the **Tasks** pane.
5. In the **Tasks** pane, expand the **HP Integrity Servers** folder.
6. Select **HP System Management Homepage** option. A new browser window opens.
7. Log in to the **HP System Management home page**.

The HP Systems Insight Manager

The HP Systems Insight Manager is used to carry out life-cycle management for systems on the domain/network. Again, HP did a good job creating this task, meaning that if there are any issues, MOM notices it first and you're then able to quickly log the hardware error into the database.

To launch the HP Systems Insight Manager task, perform the following steps:

1. Open the **MOM Operator console**.
2. Select **Public View**.
3. Select a computer from the **Computers** view under the **HP ProLiant Servers** folder or the **HP Integrity Servers** folder.
4. Select the **Tasks** button on the menu bar to display the **Tasks** pane.
5. In the **Tasks** pane, expand the **HP ProLiant Servers** folder or the **HP Integrity Servers** folder.
6. Select **HP Systems Insight Manager**. A new browser window opens.
7. Log in to **HP Systems Insight Manager**.

The HP Lights-Out Management Processor

The HP Management Processor task is only available if the HP Integrity servers are deployed on the network. Using this task will open a Web interface on the server that enables you to perform hardware security and maintenance online. This task has the same function as the Precision task in the HP Management Processor.

To launch the HP Lights-Out Management Processor task, perform the following steps:

1. Open the **MOM Operator console**.
2. Select **Public View**.
3. Select a computer from the **Computers** view under the **HP ProLiant Servers** folder.
4. Click the **Tasks** button on the menu bar to display the **Tasks** pane.
5. In the **Tasks** pane, expand the **HP ProLiant Servers** folder.
6. Select **HP Lights-Out Management Processor**. The **Launch Task Wizard** opens.
7. Click **Next**.
8. Click **Next** when prompted to edit the command-line task parameters. The default command-line entry should not require editing.
9. Verify that the computer listed in the **Targets** pane is the correct server, and then click **Next**.
10. Click **Finish**.

11. Select **Task Status** under the **HP Integrity Servers** folder from **Public Views**.
12. Locate and select the task launched.
13. Select the **Properties** tab on the **Event Details** pane.
14. Select the hyperlink to open a browser interface to the HP Management Processor on the associated HP Integrity server.

Computer Model Discovery

The computer model task is used to discover and classify the HP ProLiant servers. This task is started using a regular schedule, but if you need to get things started manually, this task will kick up the discovery process.

To launch the Discovery task, do the following:

1. Open the **MOM Operator console**.
2. Select **Public View**.
3. Select a computer from the **Computers** view under the **HP ProLiant Servers** folder.
4. Click the **Tasks** button on the menu bar to display the **Tasks** pane.
5. In the **Tasks** pane, expand the **HP ProLiant Servers** folder.
6. Select **Discovery** to expand the contents, and then choose **Service Discovery**. The **Launch Task Wizard** opens.
7. Click **Next**.
8. Verify that the computer listed in the **Targets** pane is the correct server, and then click **Next**.
9. Click **Finish** to perform the server discovery and populate the appropriate HP computer groups.

Managing Dell Servers

Another great server brand is Dell. Dell is also one of the first vendors that recognized the power of MOM in a network and were quick to release the Dell management pack for MOM 2005. It actually goes beyond the components of the system in that it also monitors the system-state—for example, a case where the server is opened enough to initiate a security alert in the operator console.

To make this all possible, you need to install the Dell OpenManage toolkit on each of the servers. Doing so will not only give you the ability to perform offline

actions while online, but it's also required for the Dell OpenManage Management Pack to work correctly.

Some Independent Advice

Currently, Microsoft has a very stable server operating system. The products that install upon these systems are mostly stable and have a high availability. One of the main concerns is the hardware and common reasons for unexpected downtime. In fact, if you research the problem afterward, you'll likely find you could have prevented the problem. This gap is where MOM can come in handy.

Note

Remember, the solutions all lie in the manufacturer-supplied server software (like Dell OpenManage and HP Insight management). Deploy this software on all servers and the MOM management pack will work directly.

Shortcuts…

When Importing the Management Pack

This is one of the first management packs you need to import. You start with the Base OS, wait for the event storm that comes after the import, and resolve the issues from that storm. Then, install the hardware monitoring pack.

An Overview of the Available Dell Management Packs

Dell Management Pack for MOM 2005

The Dell Management Pack for MOM 2005 is the first Dell OpenManage management pack and can only be used in a MOM 2005 environment. It offers a rich set of monitoring functions and runs like a charm. It monitors the Power Edge series, and, if connected, the Dell PowerVault SAN series of Dell.

Since it's available on the Microsoft Management Pack Web site, it fulfills the requirements that Microsoft has for third-party management packs. One of those requirements is the addition of knowledge in the database. This way, the users of MOM not only know what went wrong, but they also know how to resolve the issue.

After importing the management pack, the Dell computers group must be visible in the MOM Operator console:

The following list of rule groups will be added to your MOM infrastructure:

- Dell OpenManage
- Dell OpenManage\Array Manager
- Dell OpenManage\Server Administrator
- Dell OpenManage\State Monitoring and Service Discovery
- Dell OpenManage\Storage Management

The Dell OpenManage Management Pack

The Dell OpenManage Management Pack is not exclusive to MOM 2005. It can be imported into MOM 2000 as well.

After importing the management pack into a MOM 2005 environment, the Dell computers group will be added to the database.

The following list of rule groups will thus be added to your MOM infrastructure:

- Dell OpenManage
- Dell OpenManage\Array Manager
- Dell OpenManage\Server Administrator
- Dell OpenManage\Storage Management

Shortcuts…

Older Management Packs

This management pack will indeed work in MOM 2005. Therefore, you can import it, but if your hardware and Dell OpenManage software already supports the Dell Management Pack for MOM 2005 management pack, there is no deed to do so. The new release (2.0) supports all functions offered in this pack, and offers additional functionality.

Third-Party Management Packs

eXc Software has a third-party product called *Virtual Agent for Dell Open Manage*. This virtual agent is used to monitor servers running another OS than Windows 2000 or Windows Server 2003 (for example, UNIX).

This is fairly uncommon in the wild since most environments monitored by MOM are Microsoft based. The Virtual Agent for Dell OpenManage protocol uses SNMP to communicate. To monitor a non-Windows environment, you need to install the eXc software non-Windows WMI event provider. After installing the WMI provider, you can then install the virtual agent, and start monitoring the server/system.

Importing the Dell Management Packs

The import of Dell management packs follows the same procedure as other management packs described in this book. However, there are a couple of prerequisites you need to be aware of.

The Dell Management Pack for MOM 2005

Again, only import the Dell Management Pack for MOM 2005 if you intend to monitor Dell PowerEdge servers. This management pack will check if the Dell OpenManage software is installed on the servers, and so will only send the rules that have this software.

The following prerequisites must be met in order for the management pack to function correctly.

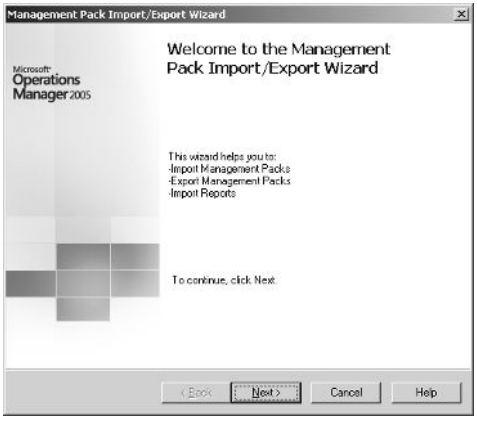
- Support for Dell OpenManage Server Administrator versions 1.6–2.0 (including the enhanced Storage Management Service version 1.0–1.1). For receiving alerts from the storage subsystem, you must have installed either Dell OpenManage Array Manager or the Server Administrator enhanced Storage Management Service.
- Support for Array Manager Versions 3.4–3.7

In most cases, the Dell OpenManage software that comes with the server is sufficient to monitor the hardware using this management pack.

To import the management pack, perform the following steps:

1. In the **Navigation** pane, click **Management Packs**.
2. In the **Detail** pane, click **Import/Export Management Packs** to open the **Management Pack Import/Export Wizard**. (See Figure 9.8.)

Figure 9.8 The Welcome Screen for the Management Pack Import/Export Wizard



3. Follow the instructions in the Management Pack Import/Export Wizard, and click **Next** to start the import operation.
4. Select **Import Management Packs and/or reports**. (See Figure 9.9.)
5. Select the location to save the file to, and then choose the Import **Management Packs Only** option. (See Figure 9.10.)

Figure 9.9 The Import or Export Management Packs Screen

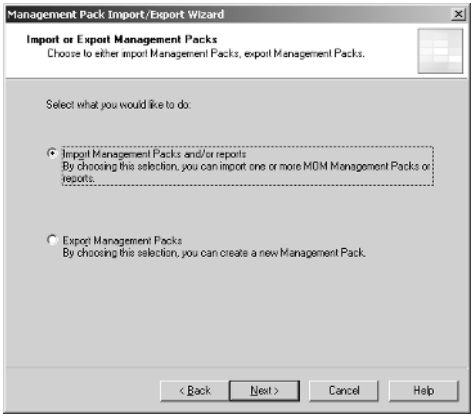
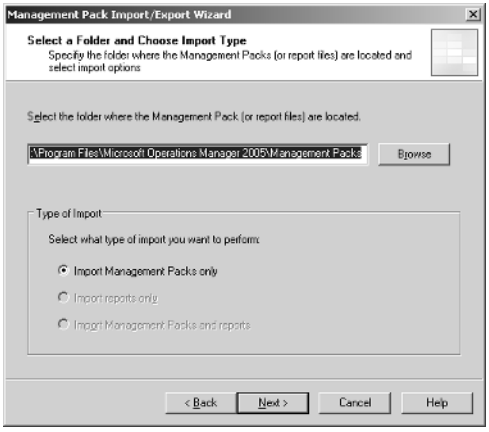
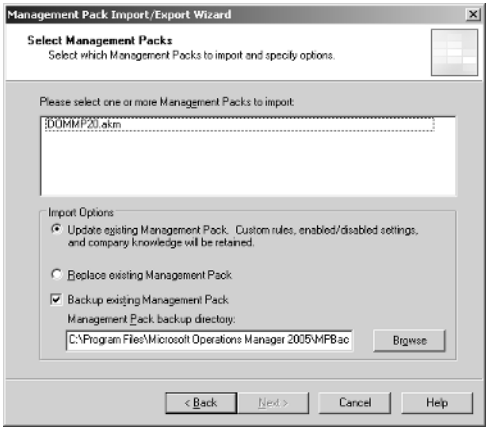


Figure 9.10 Select the Folder Where the Management Pack Is Located



6. Click **Next** to launch the **Selection** screen.
7. Select each Management Pack to import, and then choose **Update.** (See Figure 9.11.)

Figure 9.11 The Select Management Packs Screen



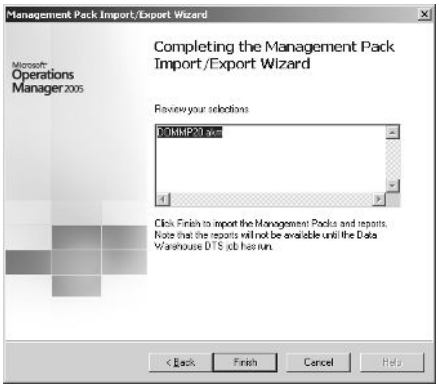
Shortcuts…

What Type of Import to Choose

There is a real need to know what type of import should be done. If you select Update, the management pack will install and add information to that management pack. If you select Replace, the management pack will be removed and the new one imported. This can be a big drawback in that all the company information stored in the management pack will be removed. Thus, again, the best option to use Update, and if that doesn't work the way you planned, use Replace.

8. Review the selections and then click **Finish** to start the import operation. (See Figure 9.12.)
9. Right-click the **Management Packs** folder on the MOM **Administrator** console, and then select **Commit Configuration Change**.

Figure 9.12 Finish Importing the Management Pack



The Dell OpenManage Management Pack

The Dell OpenManage Management Pack can be used only if Management Pack 2.0 isn't supported.

Prerequisites for this management pack include the following:

- Supported Dell OpenManage Server Administrator versions: Server Administrator versions 1.0–1.9
- Supported Dell OpenManage Array Manager versions: Array Manager versions 3.1.1–3.6

Repeat the same steps as outlined in the earlier section on importing Dell management packs, "Dell Management Pack for MOM 2005."

Configuring and Using the Dell Management Packs

Dell uses the Hardware Support notification group. This notification group should be populated with those engineers that do hardware support.

This is the only post configuration that needs to be done to successfully import and run the Dell OpenManage Management Pack.

Summary

Hardware monitoring is essential in providing the best availability possible. A couple of vendors publish a management pack at the Microsoft site: The HP management pack supports the HP Integrity and HP ProLiant series servers, and the Dell Management Pack supports the PowerEdge series server. The implementation of these management packs depends on the installation of the vendor-supplied management software.

In this chapter, we took a closer look at how to monitor Intel-based hardware. Using hardware monitoring, we were able to discover hardware failures that otherwise wouldn't show up in the MOM Operator console. An example of this would be the failing of a single disk in a Hardware-Raid. We discussed the HP and Dell Management Packs and how to import them into MOM.

Solutions Fast Track

Managing Server Hardware

- ☑ Many errors come from hardware failures, much of which could be prevented if noticed at an early stage.
- ☑ The Base OS Management Pack is one of the core management packs and is, in most cases, essential for a successful deployment.
- ☑ After importing the Base Server OS Management Pack, little or no configuration is needed.
- ☑ If you run into issues regarding disk space checks, you should be able to tweak the minimum allowed space on the OS level.

Managing Intel-Based HP Servers

- ☑ Only import this management pack if you intend to monitor HP servers.
- ☑ Three versions exist—the HP Insight Management Pack, the HP Integrity Management Pack, and the HP ProLiant Management Pack.
- ☑ The HP Insight Management Pack is outdated, so if you have no explicit reason to import it, use the MOM 2005 version.

- ☑ The HP Integrity Management Pack is intended for the HP Integrity Server series.
- ☑ The HP ProLiant Management Pack is intended for the HP ProLiant Server series.

Managing Dell Servers

- ☑ Only import this management pack if you intend to monitor Dell servers.
- ☑ Two versions are available—the Dell OpenManage Management Pack and the Dell Management Pack for MOM 2005.
- ☑ The Dell OpenManage Management Pack (version 1.2) is outdated and should not be used if there's no explicit reason to do so.
- ☑ The Dell Management Pack for MOM 2005 is intended for the Dell PowerEdge server and Dell PowerVault mini-SAN series.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: I want to monitor my servers, but they're not from Dell or HP. What should I do?

A: If your server vendor is Fujitsu Siemens, there's an additional management pack available that's not covered in the book. If the hardware isn't from any of these vendors, you're headed down a bumpy road. You could use WMI to access the status information of the servers. But to use it, the server software should support the WMI classes in order to access the hardware.

In short, if your server isn't from Dell, HP, or Siemens, you'll have a hard time setting up the rules.

Q: I have a server with five disks in a RAID array. Will MOM monitor the availability and fire an alert over e-mail or page in case an HDU fails?

A: This depends on the configuration of the rules. If the alert rule has a response rule that sends a notification, you can enable the receiving of the notification. You can do this by adding a mail- or page-enabled operator in the notification group that's alerted.

Q: If I use Replace instead of Update when installing a management pack, is there any way for me to recover my data?

A: The management pack restoration depends on the options selected during the replacement process. If you selected the Back Up Existing Management Pack option during the replacement, there's no real harm done. Just replace the newly imported management pack with the old one and start over in Upgrade mode. If you didn't select the Back Up Existing Management Pack option, you have a bigger problem. All custom information is overwritten and can only be restored using a backup of the database. Restoring this information will result in the loss of event and performance data.

Q: Are there any plans to have the Base OS Management Pack monitor Windows Vista?

A: According to Microsoft's latest statement, they will probably offer support for Vista in MOM 2005. Microsoft is committed to deliver support in MOM for every mayor release within six months. This can come by way of a new management pack, or through the upgrade of an existing one.

Q: I have some older Compaq ProLiant servers (an 1850, for example). Will the HP management pack support this?

A: One of the things you need to find out is the insight manager software version that is available for these systems. If you're able to run a version supported by either of the two management packs available for HP/Compaq servers and you're running Microsoft Windows NT 4.0 or later, you should be able to monitor the system.

Q: I have multiple Windows NT 4.0 servers that don't have enough free space to pass the free space threshold rule so MOM is firing alerts on them. How can I make MOM monitor the server of just one individual base?

A: This is difficult to do. One option is to edit the free space script and create your own rule, but this isn't the easiest method. A better way is to set an absolute

minimum for the Windows NT 4.0 operating system and then edit the rule as described in this chapter.

Chapter 10

Managing Linux, UNIX, and Solaris

Solutions in this chapter:

- **Agentless Management of Linux and UNIX Servers**
- **Agent-based Management of Linux and Solaris Servers**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

The degree to which you can integrate non-Windows systems into MOM 2005 depends on what technique you use to manage that resource. To collect a sufficient amount of data to drive MOM's alert system, custom providers (using the MOM 2005 SDK) are needed to interact with the instrumentation exposed by the operating system as well as accompanying management packs with the associated event and alert rules. Third-party software vendors have developed solutions to extend the functionality of MOM into the non-Windows arena. In this chapter, we will look at two different approaches to managing non-Windows resources, agentless and agent-based.

Agentless Management of Linux and UNIX Servers

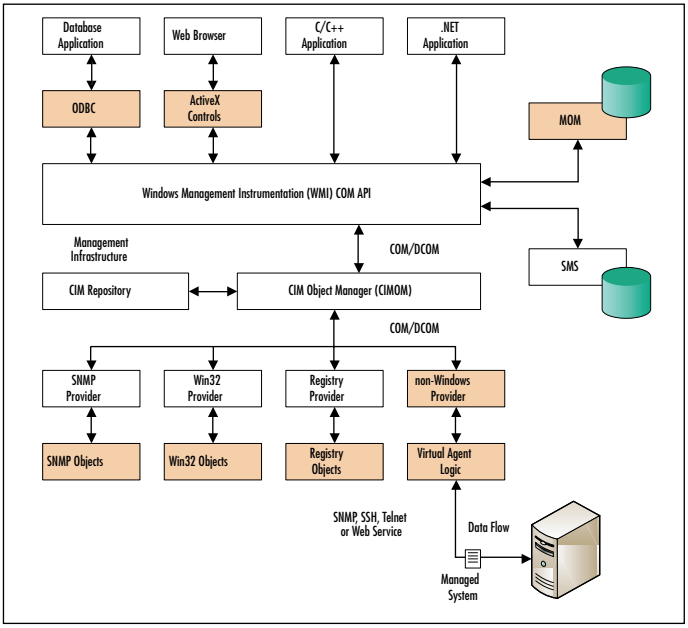
The first method of managing non-Windows systems is to use Virtual Agents to collect state and performance data from those resources. When using Virtual Agents, there is no need to deploy any software on the managed systems. Instead, calls to the systems to capture data or invoke an action are made using common interfaces supported by the managed systems.

Overview of Virtual Agents

Infrastructure and application monitoring is shifting from an agent-based approach to an agentless one. Agentless monitoring holds the promise of cheaper and easier-to-maintain monitoring technology. Only a few technology barriers still exist thanks to emerging technologies and adoption by both operating system and application vendors. One company breaking those barriers by extending MOM's management capabilities for heterogeneous environments is eXc Software.

eXc Software provides an extensive library of Virtual Agents that utilize a custom-developed Windows Management Instrumentation (WMI) Event Provider to deliver event and performance data to MOM. Figure 10.1 shows the component architecture for the eXctender WMI Event Provider. eXc Software's WMI non-Windows Event Provider is a component DLL that runs within the WMI service. WMI is Microsoft's implementation of a set of standards that has been established by the Distributed Management Task Force (DMTF). Those standards make up the Web-Based Enterprise Management (WBEM) technologies whose goal, in theory, is to unify the management of distributed computing environments and allow an IT organization to monitor and control all the systems found within its data centers.

Figure 10.1 The Component Architecture for the eXctender WMI Event Provider



eXc Software has taken a unique architectural approach by utilizing simple yet powerful scripting languages to exploit the inherent capabilities of WMI. The Virtual Agents are a collection of scripts (either JScript or VBScript) that utilize COM objects to access Linux and UNIX systems. Those objects provide the ability to establish sessions and communicate with the managed systems using SSH, Telnet, SNMP, or Web services. Through the rich set of features provided by these scripts and COM objects, you can perform automation tasks on all your Linux or UNIX systems.

Virtual Agents for Linux and UNIX

eXc Software has an extensive library of out-of-the-box Virtual Agents for most of the popular Linux distribution, including Red Hat, SuSe, Mandrake, Debian, and FreeBSD. In addition, eXc Software also provides Virtual Agents for UNIX versions, such as Solaris, AIX, and HP-UX. Although each Virtual Agent is customized, or tweaked, to function properly with the system running that particular operating system, they all are the same in form and function. Most of the differences in the various Virtual Agents for Linux and UNIX revolve around format differences from the extracted output returned from certain commands such as *df*, *ps*, *top*, and *vmstat*. Another difference is how the Virtual Agent auto-discovers the system. In fact, the differences are so subtle,

you can easily take any of the Virtual Agents and make minor modifications to tailor it to a distribution or version not yet available from eXc.

Regardless of which Virtual Agent you are going to use, you must install the eXc Software's WMI Event Provider. All of the eXc Software Virtual Agents share this single common base framework. Once the framework has been installed, you will be able to add any of the Virtual Agent solutions.

Anatomy of a Virtual Agent

An eXc Software Virtual Agent is a collection of files that are composed of several scripts (both VBscript and JScript), configuration files, and text files. A Virtual Agent is installed from an MSI package and all its files are located in a single directory, commonly under the Virtual Agent Library\MOM folder where the base framework was installed. Table 10.1 explains each file type and its role in the Virtual Agent.

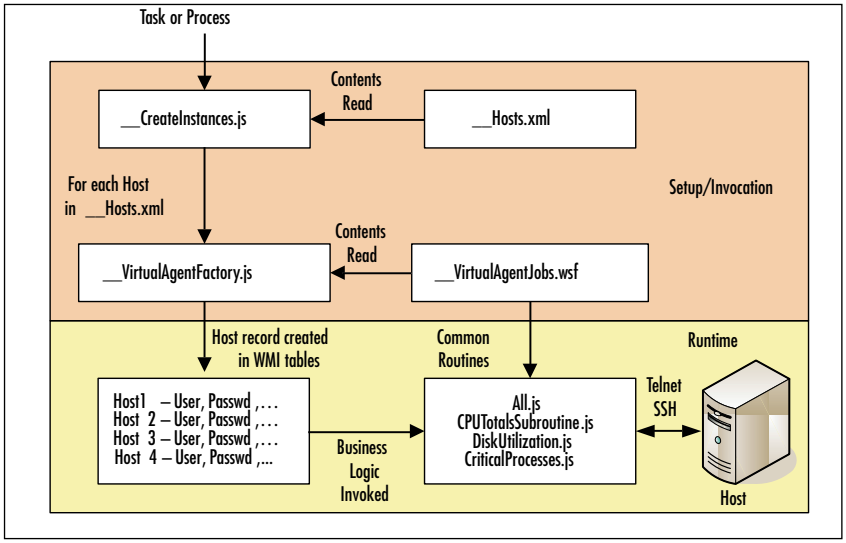
Table 10.1 Virtual Agent File Type and Role

File Type or Name	Role or Function
__CreateInstances.js __VirtualAgentFactory.js __Hosts.xml __Hosts.csv __VirtualAgentJobs.wsf	Those files that begin with two underscores are used to create the Virtual Agent. This invoked agent also is referred to as the Factory.
All other VBS and JS files	These files implement the "business logic" of the Virtual Agent.
All other XML files	The XML files contain the data used by the Virtual Agent's business logic. This data represent the tailored configuration of the Virtual Agent, including thresholds, processes that the Virtual Agent should monitor, log files to monitor, etc.
TXT files	These files contain encrypted USERID and PASSWORD information (optional).

Although understanding all these files and what they each do may appear complicated, Virtual Agents actually follow a simple workflow, as shown in Figure 10.2.

The process all begins when the eXc Software WMI Event Provider is loaded after starting the WMI service. The WMI Event Provider then starts each Virtual Agent using the following process:

Figure 10.2 High-Level Workflow of Virtual Agent Invocation and Runtime



- Calls the Virtual Agent's **__CreateInstances.js** script. This script reads the **__Hosts.xml** file to identify the systems to be managed by the Virtual Agent.
- For each host record, the **__VirtualAgentFactory.js** script is called. This script is passed the appropriate information about each host, including the DNS host name, login information or the filename and path containing the encrypted login credentials, what port to connect with, whether to use SSH or Telnet, and whether or not to run Watchdog (a monitoring process that is used to control CPU utilization).
- Host information passed to the **__VirtualAgentFactory.js** script is populated into the WMI tables, which define the host to WMI.
- Once the WMI host object is stored, WMI will begin to execute the business logic scripts. Although the business logic scripts contain custom routines for each management function, such as monitoring critical processes or collecting disk utilization statistics, common routines are shared between each script rather than being loaded when each individual script is run. This is accomplished by utilizing Microsoft's WSF environment, defined in **__VirtualAgentJobs.wsf**.

SNMP versus CLI-Based Virtual Agents

It is worth noting at this point that there are two types of Virtual Agents—those that use SNMP for managing the non-Windows resource and those that use a Command-Line Interface (CLI), such as SSH or Telnet, to manage resources. Each type of Virtual Agent is catered to a particular data set of function in the overall management strategy for managing your Linux or UNIX systems.

The canned eXc Software SNMP-based Virtual Agents take advantage of the native WMI SNMP Provider available on the MOM management server. Although MIB files are not required, using them to properly interpret the SNMP message for each OID received is recommended.

CLI-based Virtual Agents utilize an automation object that supports Telnet and SSH connections to a remote system. Using the settings configured with each host record, each Virtual Agent follows a simple pattern once called from WMI via the eXc Software WMI Event Provider. Each call is passed specific parameters from the WMI tables established by the Virtual Agent factory. The typical process for each Virtual Agent, once called, includes the following steps:

1. Connect to and log into the managed system.
2. Issue commands and get the results of the commands.
3. Log out.
4. Parse those results and process the data.
5. Create an event in WMI that will get forwarded to MOM.

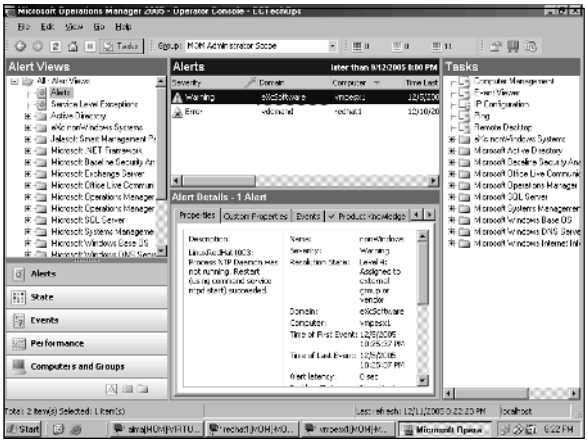
By default, each of the Linux/UNIX Virtual Agents monitors and creates MOM 2005 alerts for:

- Tail'd syslog file based on user-defined search strings
- CPU usage per process
- Total CPU usage
- Disk utilization
- Process state monitoring for specific user-defined processes. This particular alert can be further configured with a correct action or response command to run, such as to restart that particular process (see Figure 10.3).

Once MOM 2005 has received the event from either an SNMP-based or CLI-based Virtual Agent, you can create specific event and alert rules to meet your monitoring and management needs for your environment. eXc Software does not provide a management pack for each Virtual Agent; instead, they have a general eXc non-

Windows Systems management pack that contains generic rules to monitor any events that are raised through the WMI framework by any installed Virtual Agent.

Figure 10.3 Example of MOM 2005 Alert Generated from Red Hat Virtual Agent



eXc Software provides three basic reports along with the general management pack. The report provides an analysis of events and alerts from the WMI non-Windows Event Provider as well as a view into performance statistics captured and forwarded to MOM 2005 from the Virtual Agents, if any.

Best Practices According to Microsoft

- eXc Software provides simple-to-use SNMP interfaces that save you from having to manually configure each of your SNMP-enabled Linux or UNIX servers into WMI. This is because each of the objects takes care of the SNMP to WMI work for you.
- Incorporate your SNMP requirements into the eXc Software Virtual Agent technology by providing MIB information to the SNMP COM object.
- To make an even more effective management solution, though, you can combine the Telnet/SSH capabilities of CLI-based Virtual Agents with the handling of SNMP data to and from your Linux or UNIX systems. Combined, these features give you unlimited monitoring and automation capabilities to seamlessly integrate your non-Windows systems into MOM.

Managing a Linux/UNIX System with Virtual Agents

In the following section, we will walk through the installation steps for a new deployment of the eXc Software non-Windows Provider and the Virtual Agent for Red Hat as well as the basic configuration of the Virtual Agent. These steps should quickly get you managing your Red Hat systems with MOM 2005.

To make the installation as smooth as possible, we will assume that all eXc Software components are being installed on a single management server in an "all-in-one" fashion. Before beginning the installation of any eXc Software components, all software requirements must be satisfied. Table 10.2 shows what components need to be installed for a base install of Windows 2000 Server and Windows 2003 Server. If you are missing any requirements, a pop-up will be displayed stating so during the software installation process. Also, if you have any previous versions (prior to September 2005) of eXc Software's components, you must uninstall those before proceeding.

Table 10.2 Software Requirements for Microsoft Windows 2000 Server and Windows Server 2003

Windows Server Version	Requirement
Windows 2000 Server	Microsoft .NET Framework 1.1 Windows Script Host 5.6 Microsoft Access 2000 or later * Connection Manager Components * Network Monitor Tools * Simple Network Management Protocol Windows Management Instrumentation SNMP Provider Microsoft MSXML 2.0 or later Internet Explorer 6.0 or later
Windows Server 2003	Microsoft Access 2000 or later * Network Monitor Tools * Simple Network Management Protocol * WMI SNMP Provider * WMI Windows Installer Provider Windows MSXML 4.0 or later

Note: "*" denotes that the component is installed through the Add/Remove Windows Components section of the Add/Remove Programs control panel applet.

Once the prerequisites are installed, you can perform the basic installation steps as follows:

1. Download the eXc Software Base Framework (or WMI non-Windows Event Provider) and the Red Hat Virtual Agent from www.excsoftware.com.
2. Install the eXc Software WMI non-Windows Event Provider using the *eXc_nonWindows_WMI_Provider.msi* Windows Installer package.
3. Select the installation folder. If you change the installation path from the default folder, you will have to make further modifications after the installation. You must select **Everyone** or you will not be able to launch any of the Virtual Agents you install (see Figure 10.4).

Figure 10.4 eXc Software WMI non-Windows Event Provider Install Wizard

4. Install the Red Hat Virtual Agent that you downloaded using the *eXc_MOM_Linux_RedHat_Virtual_Agent.msi* Windows Installer package. Remember that if you changed the default install path for the event provider, you'll need to adjust the path for the Virtual Agent install folder as well. You must select **Everyone**, just as you did with the event provider install.

Importing the eXc Software Management Pack and Reports

Once all the components have been installed, you must integrate eXc Software's Event Provider with MOM 2005 as well as configure the Red Hat Virtual Agent.

Carefully perform the following post-installation steps, being sure not to skip any step to ensure proper configuration of your Virtual Agent.

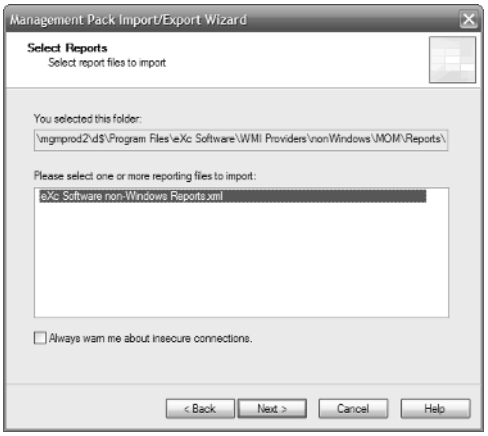
1. Using the MOM 2005 Administrator Console, highlight **Management Packs** then right-click and select **Import/Export Management Pack** to launch the Management Pack Import/Export Wizard.
2. On the Welcome page, click **Next**.
3. Select **Import Management Packs and/or reports** and click **Next**.
4. Set the appropriate directory path where you installed the WMI non-Windows Provider for MOM. By default this path is c:\Program Files\eXc Software\WMI Provider\nonWindows\MOM\.
5. Select **Import Management Packs only** and click **Next**.
6. Select the Management Pack for MOM 2005. Be sure to select the AKM file for MOM 2005.
7. Since this is a new deployment of the Management Pack, select **Replace existing Management Pack** and uncheck **Backup existing Management Pack** under Import Options (see Figure 10.5). Click **Next**.

Figure 10.5 Management Pack Import Wizard and eXc Software AKM Files

8. Click **Finish** to begin the import process and monitor the import status. Once the import process is complete, close the import window.
9. From the Select a Folder and Choose Import Type page, set the folder path to the ..\nonWindows\MOM\Reports folder.

10. Select the **Import Management Packs and/or reports** radio button and click **Next**.
11. Select **Import reports only** and click **Next**.
12. Select the *eXc Software non-Windows Reporst.xml* file to import.
13. Uncheck **Always warn me about insecure connections** (see Figure 10.6).

Figure 10.6 Importing the eXc Software Report Definition



14. Click **Next** to begin the import process and monitor the import status.
15. Once successfully imported, close the import status window.

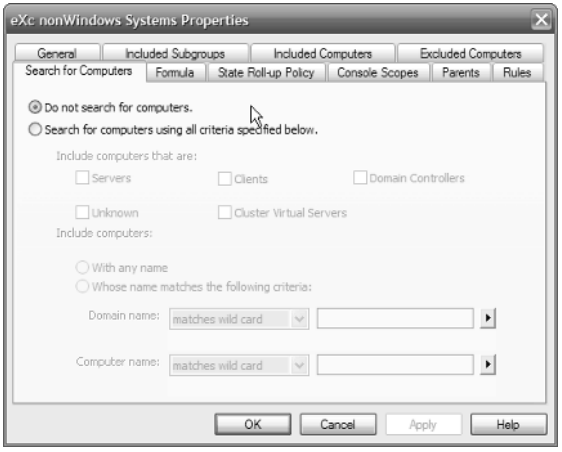
Configuring the Non-Windows Computer Group and Provider

Now that the Management Pack and Reports for eXc Software have been successfully imported, we need to configure them. You must perform the following basic steps to configure the computer group and provider created by the eXc Software management pack.

1. From the MOM 2005 Administrator Console, expand **Management Packs** and **Computer Groups**.
2. Highlight **eXc nonWindows Systems**, then right-click and select **Properties**.
3. Click the **Search for Computers** tab.

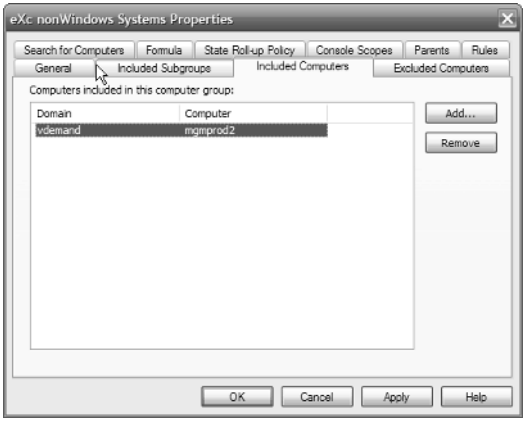
4. Select **Do not search for computers** and click **Apply** (see Figure 10.7).

Figure 10.7 Search Configuration for eXc Non-Windows Systems Computer Group



5. Click the **Included Computers** tab.
6. Click **Add** to open the Add Computer window.
7. Expand the domain where the MOM 2005 management server with the eXc Software components resides.
8. Click on the name of the management server and then click **OK**.
9. You should see the MOM management server now listed on the Included Computers tab. Click **Apply** then click **OK** (see Figure 10.8).

Figure 10.8 Configuring Management Server as eXc Single Point of Reference



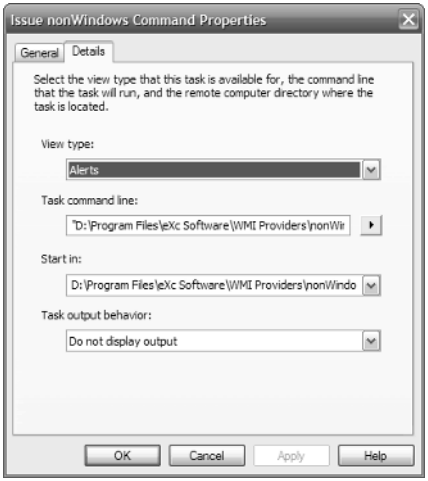
10. On the left pane of the MOM 2005 Administrator Console, expand **Management Packs** and click **Providers**.
11. Locate the WMI Events provider named *eXc_nonWindows_WMI_Provider* in the right pane.
12. Double-click **eXc_nonWindows_WMI_Provider** to open the Properties window.
13. Be sure that Namespace is set to *\\.\root\cimv2*. Click **OK**.

Configuring the Non-Windows Tasks

If you changed the default installation path for the eXc Software provider, you must alter the path reflected in the tasks created by the eXc Software management pack as explained in the following steps. If you did not change the installation folder from the default path, you do not need to complete these steps.

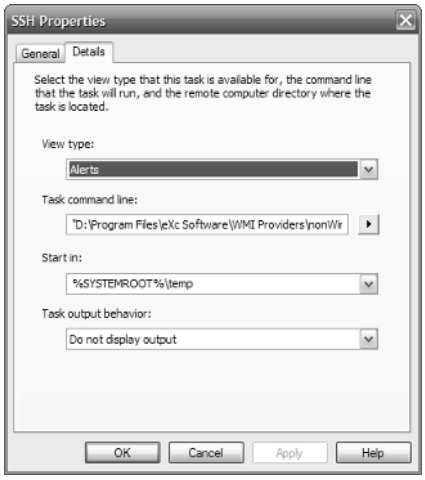
1. On the left pane of the MOM 2005 Administrator Console, expand **Tasks** and highlight **eXc non-Windows Systems**.
2. On the right-pane, double-click **Issue nonWindows Command** to open the Properties window.
3. Click the **Details** tab.
4. Adjust the **Task** command line and **Start in** parameters to reflect the correct drive and folder path (see Figure 10.9).

Figure 10.9 Adjusting Parameters for Issue Non-Windows Command Task



5. Click **OK**.
6. On the right pane, double-click **SSH** to open the Properties window.
7. Click the **Details** tab.
8. Adjust the **Task** command line to reflect the correct drive and folder path (see Figure 10.10). By default, this path points to the PuTTY SSH client included with the eXc Software installation. If you prefer, you can install another SSH client and reference the path to its executable here instead.

Figure 10.10 Adjusting Parameters for SSH Task

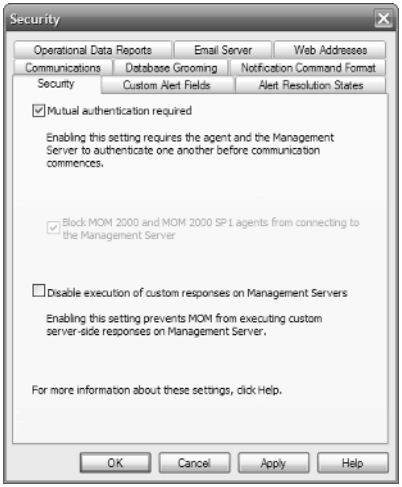


Configuring Security

The eXc Software components rely on execution of responses on the management server where you installed the software. However, by default, MOM 2005 does not allow custom responses to be executed on management servers, only on management agents. You must adjust the global security settings for MOM 2005 to allow the framework components to function properly on the management server. The following steps demonstrate the changes to the global settings needed.

1. On the left pane of the MOM 2005 Administrator Console, expand **Administration** and highlight **Global Settings**.
2. Double-click **Security** in the right pane.
3. Uncheck **Disable execution of custom responses on Management Servers** (see Figure 10.11).

Figure 10.11 Enabling Custom Responses on Management Servers



4. Click **OK**.

Completing the Installation

To complete the configuration, you must commit the changes that you have made in the previous steps. To accomplish this:

1. Right-click on **Management Packs** in the left pane.
2. Select **Commit Configuration Change**.
3. Close the pop-up message.
4. Close the MOM 2005 Administrator Console.

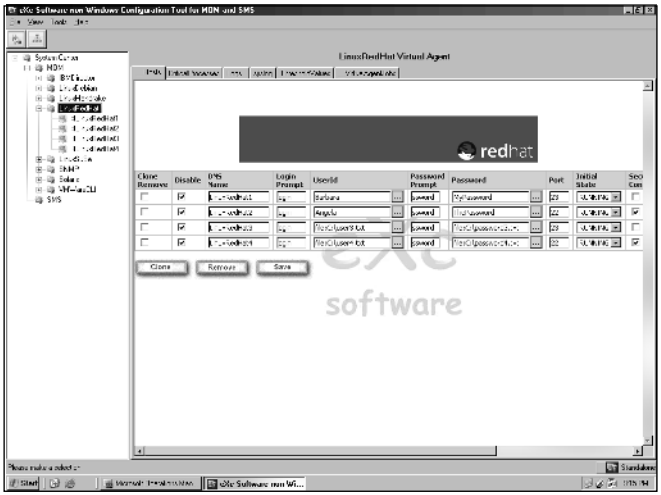
Configuring the Virtual Agent

At this point, the MOM 2005 integration is complete and the eXc Software base framework has been configured. The next step is to configure the Red Hat Virtual Agent using the eXc Software Configuration Tool/GUI. The following steps outline the tasks that must be performed to configure the basic functionality of the Red Hat Virtual Agent.

1. Run the eXc Software Configuration Tool/GUI. It can be launched from Start \Programs\eXc Software\WMI Providers\nonWindows\ Configuration Tool.

2. Expand **System Center** and **MOM**. You'll see the LinuxRedHat Virtual Agent listed (along with any other Virtual Agents that may have been installed as well).
3. Expand and highlight **LinuxRedHat**. You will find four sample targets on the right pane already listed, denoted with the naming convention #LinuxRedHat (see Figure 10.12).

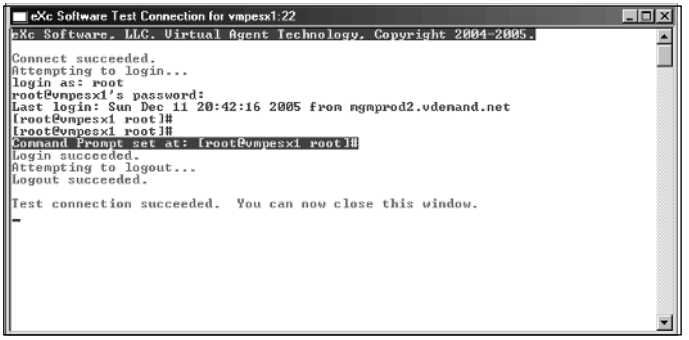
Figure 10.12 Initial Settings for the Red Hat Virtual Agent



4. Select the **__Hosts** tab.
5. Check the checkbox in the **Clone/Remove** column for the last three samples and click **Remove**.
6. In the remaining row, enter the host name (not the FQDN) in the **DNS Name** column.
7. Enter the login credentials the Virtual Agent should use. You can leave the default values for the **Login Prompt** and **Password Prompt**. Those value are to assist the TelnetAutomation object (discussed later) in recognizing the lines with login and password prompts. If you are concerned about having this information display in clear text, you can also browse to and select an encrypted text file with that information.
8. Enter the port the Virtual Agent should use to connect Red Hat system and whether the connection should be secure or not. These settings will depend on whether the Virtual Agent will use Telnet (**Port** set to 23 and **Secure Connection** unchecked) or SSH (**Port** set to 22 and **Secure Connection** checked).

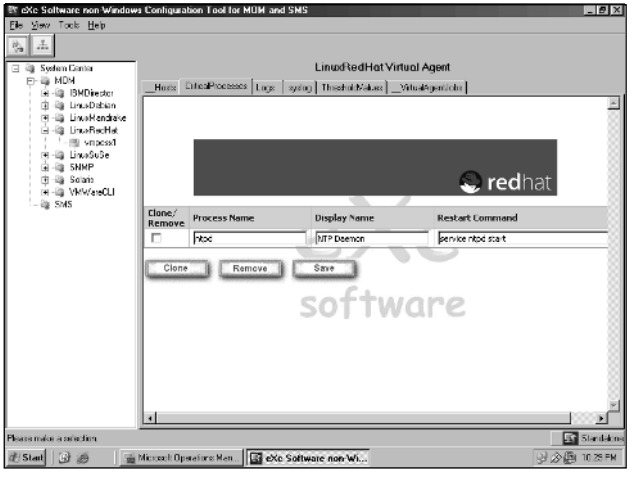
9. Leave the remaining columns with their default values.
10. Click **Save**.
11. Test the configuration by right-clicking the Host and selecting **Test Connection** (see Figure 10.13).

Figure 10.13 Results from a Successful Connection Test



12. Select the **CriticalProcesses** tab.
13. By default there are two sample processes to monitor. Modify the **Process Name**, **Display Name**, and **Restart Command** columns to reflect the processes that you want to monitor (see Figure 10.14).
14. Click **Save**.

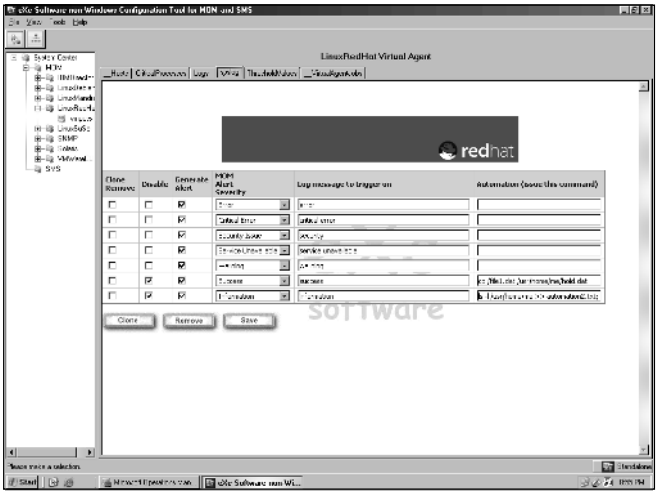
Figure 10.14 Setting up Critical Processes with Corrective Action



15. The next two tabs are used to configure syslog monitoring on the Red Hat system. Click the **Logs** tab.

16. Modify the **File Name** path, if necessary, to reflect the correct path of the syslog file. By default, the Red Hat syslog is located at /var/log/messages.
17. Click **Save**.
18. Click the **syslog** tab.
19. Configure the syslog alerting parameters. The primary field is **Log message to trigger on**. When the string that you enter here is encountered in the syslog, an alert will be generated in MOM 2005 at the Severity level you set here as long as the **Generate Alert** field is checked and the row is not disabled (see Figure 10.15). Additionally, you can run a particular command on the Red Hat system when the alert is generated.
20. Click **Save**.

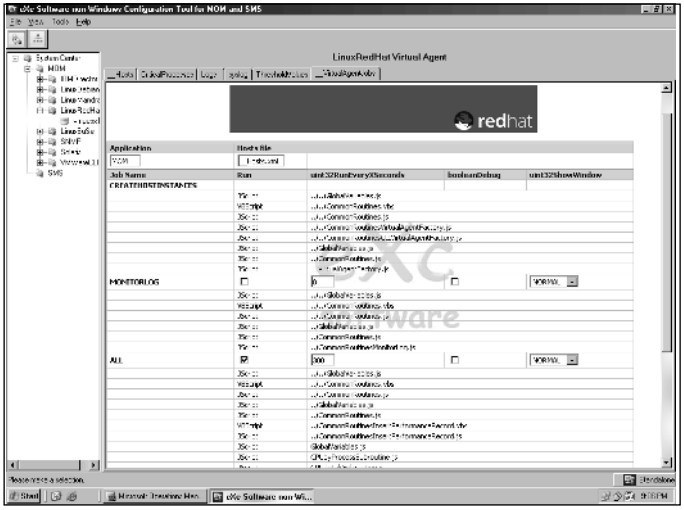
Figure 10.15 Alert Configuration for SYSLOG



21. Click the **Threshold Values** tab.
22. Set the value for each utilization performance counter listed. When the threshold is passed, an alert will be generated in MOM.
23. Click **Save**.
24. Click on the **__VirtualAgentJobs** tab.
25. This tab shows all the jobs that are run by the VirtualAgent, including which scripts are executed with each job. The jobs that you may want to customize are ALL and LOGS. By default, they are both set to run every 600 seconds, or every 10 minutes. Adjust this value to suit your monitoring needs. In addition, you can define whether the script's window is hidden,

minimized, maximized, or displayed in a normal size each time the scripts run (see Figure 10.16).

Figure 10.16 Job Definition for Virtual Agents



26. Click **Save**.

With all the components now fully installed and the configuration complete, you must reload the Windows Management Instrumentation and restart MOM 2005 on the management server. Simply use the Services administrative tools and restart the WMI and MOM services. The eXc Software is ready to start monitoring your Red Hat system. To begin the monitoring processes, use the eXc Software Configuration Tool, expand the left pane until you see your Red Hat system's name, and then right-click on it and select **Start**. The icon next to the name should turn green indicating that the Virtual Agent is now monitoring that system. Several jobs will also begin to run in command shell windows once the Virtual Agent starts up.

Customizing the Virtual Agent

Getting more out of the Virtual Agents or creating your own Virtual Agent is not difficult if you have a good understanding of COM objects and one of the many scripting languages supported by Microsoft's operating systems. Once you decide whether you want to use SNMP or CLI commands to manage your non-Windows system, you can get started with the many samples and templates that eXc Software provides in the product and on their Web site.

SNMP-Based Virtual Agent Customization

SNMP-based Virtual Agents are composed of a suite of objects that handle standard SNMP Get and Set commands to the managed system, all the SNMP to WMI processing including MIB parsing, and creating SNMP traps and forwarding them on to the configured trap destination or network management system. Those objects are listed in Table 10.3.

Table 10.3 eXc Software SNMP COM Objects

COM Objects	ProgID and Description	Members
TrapCatcher	**TrapCatcher.TrapCatcherInterface**	Initialize
	This COM object receives SNMP V1 and V2 Traps.	GetTrap2
TrapThrower	**TrapThrower.TrapThrowerInterface**	Initialize
	This COM object throws SNMP V1 and V2 Traps.	Add SNMPField toTrap ThrowSNMPTrap2
GetterSetter	**SNMPGetterSetter.** **SNMPGetterSetterInterf**	Initialize Get
	This COM object gets and sets SNMP OIDs from an SNMP-capable device.	Set
CollectionObject	**CollectionObject.** **TheCollectionObject**	Insert Clear
	This COM object is a container (collection) of SNMPFieldItem objects (SNMP OIDs).	Item Count Remove
SNMPFieldItem	**SNMPFieldItem.** **SNMPFieldItemInterface**	SNMPName SNMPOID
	This COM object exposes properties of an SNMP OID.	SNMPType SNMPValue

Your SNMP Virtual Agent can interact with MOM 2005 just like any other Virtual Agent. You can call the WMI Event Provider for non-Windows SendEvent method (SendEvent gets wrapped by the Virtual Agent common library routine ThrowAlert) to have the SNMP data processed by MOM and perform a response, such as generating an alert, sending a notification via e-mail or pager, or run a program. You can also invoke the methods in the MOM WMI classes included with the MOM 2005 SDK, such as the MSFT_Computer_Class.

The following example includes a script that catches SNMP traps and uses the eXc Software SNMP COM object TrapCatcher. In this example, the TrapCatcher object is passed the MIB for Intel network adapters, which is passed to the TrapCatcher object. The script runs in an infinite loop, waiting for a trap to be received. Once one is picked up, the script writes out the name and value of for each property exposed by the MIB.

Code Sample of SNMP TrapCatcher Object

```
var l_strReadSNMP = "public";
var l_strMibDir = "C:\\ mibs";
var l_strMib = "intelnic";
var strName_in = "Server01";

var l_objTrapCatcher = new
ActiveXObject("TrapCatcher.trapCatcherInterface");
l_objTrapCatcher.Initialize(strName_in, l_strReadSNMP, l_strMibDir,
l_strMib);

for (i=0;i>-1;i++)
   {
   WScript.Echo("Collecting SNMP Traps for " + strName_in + "; counter=" +
i);
   var l_objTrap = l_objTrapCatcher.GetTrap();
   if ("undefined" != typeof l_objTrap)
      {
      var l_Enumerator = new Enumerator(l_objTrap);
      var l_intPropertyCounter = 0;
      for (;!l_Enumerator.atEnd();l_Enumerator.moveNext())
         {
         var l_objSNMPField = l_Enumerator.item();
         var l_strName = l_objSNMPField.SNMPName;
         var l_strOID = l_objSNMPField.SNMPOID;
         var l_strType = l_objSNMPField.SNMPType;
         var l_strValue = l_objSNMPField.SNMPValue;
         WScript.Echo(l_strOID + "(" + l_strName + ") = " +
             l_strValue + " of type " + l_strType;
         }
      l_Enumerator = null;
   }
```

CLI-Based Virtual Agent Customization

To work with your Linux or UNIX systems using CLI protocols, such as Telnet and SSH, you instantiate a COM object provided by eXc Software object within your own script code. This object, called the TelnetAutomation object, provides a group of methods and properties to connect to a managed device or system, login and logoff, key commands, collect the results, and check connection and command status, as listed in Table 10.4.

Table 10.4 List of the APIs for the TelnetAutomation Interface

Members	Description
AutoStart	This method will call methods PopulateProperties, connect, and login for you.
Clear	This method will clear the screen buffer. Note that any bookmarks you have will become invalid.
Connect	This method is used to establish the Telnet or SSH connection to the host specified in property stringHostName.
connectCheck	This method will check if a Telnet or SSH connection to the host specified in property stringHostName can be made. This method is used by the Auto-discovery utility but could be used by any program.
getDataBufferLength	This method returns the current number of lines in the data buffer.
getData	This method will return lines of data from the telnet or SSH session screen buffer, starting at line longFrom_in to the current last line of the Telnet or SSH session. The Telnet or SSH screen buffer is converted into one big string starting at longFrom_in to the bottom.
getDataAsSafeArray	This method will return lines of data from the Telnet or SSH session screen buffer, starting at line longFrom_in to the current last line of the Telnet session in the form of an unmanaged safe-array.

Continued

Table 10.4 continued List of the APIs for the TelnetAutomation Interface

Members	Description
getOneLineOfData	This method will return one line of data from the Telnet or SSH session screen buffer at the line specified by longFrom_in. If longFrom_in is greater than the last current line, then getOneLineOfData will wait for longWaitTimeInMilliseconds_in milliseconds and then return back to the caller with a zero length string. This method is particularly useful if, for example, the caller is "tailing" on a file and the caller does not know when the next line will be displayed.
Key	This method will send keystrokes to the Telnet or SSH session. You do not need to specify a carriage return as the key method will do it for you automatically.
Login	This method will login to the Telnet or SSH connection of the host specified in property stringHostName Be sure that you have 1) set the stringUserName property, 2) set the stringPassword property, 3) have successfully called the connect method before you call the login method.
Logout	This method will logout of the Telnet or SSH connection of the host specified in property stringHostName. You should have already called method login before you call the logoff method.
PopulateProperties	This method will populate the following properties: stringHostName, stringLoginPrompt, stringUserName, stringPasswordPrompt, stringPassword, stringHostPort, boolSecureConnection, and boolIsPingable from the WMI Event Provider for non-Windows.
respondTo	This method will reply to an input prompt by looking for the string stringRequestString_in from the telnet or SSH session starting at line longFrom_in and when it is found, it will key in the string stringReplyString_in. This method will look for the string stringRequestString_in

Continued

Table 10.4 continued List of the APIs for the TelnetAutomation Interface

Members	Description
	for longWaitTimeInMilliseconds_in milliseconds and if does not find string stringRequestString_in within longWaitTimeInMilliseconds_in milliseconds, it will return an error to the caller.
boolArePropertiesPopulated	This flag indicates whether the WMI Event Provider for non-Windows populated the properties successfully or not.
boolIsConnectedToHost	This flag indicates whether you are connected to the host. This field should be checked after you issue the connect method.
boolIsLoggedInToHost	This flag indicates whether you are logged in to the Telnet host. This field should be checked after you issue the login method.
boolIsPingable	This flag indicates whether you want the TelnetAutomation object to perform a ping test before it attempts to login.
boolSecureConnection	This flag indicates whether you are connected to the host via Telnet (value is false) or SSH (value is true).
boolWaitForKeyCommand ToComplete	This flag indicates whether the key commands will wait for all of the output to be displayed/collected (which is indicated by the last displayed/collected output line being the command prompt) before returning control back to the caller.
stringCommandPrompt	This method will get or set the current command prompt. Note that by default, the login process will initially set this property for you.
stringHostName	The DNS Host Name or IP Address of the non-Windows system the Telnet or SSH session will connect to.
stringHostPort	The port the Telnet or SSH session will connect to.
stringLoginPrompt	The login prompt string of the Telnet or SSH session.

Continued

Table 10.4 continued List of the APIs for the TelnetAutomation Interface

Members	Description
stringPassword	The password used to login to the Telnet or SSH session of the non-Windows system or device. For security reasons, you can encrypt the password into a file and then set the stringPassword as the name of the file prefixed by "file:".
stringPasswordPrompt	The password prompt string of the Telnet or SSH session.
stringTerminalType	This field allows you to negotiate a terminal type with the Telnet server. The default is vt100. If you are working with an older Telnet server, specify a zero length string. Doing so will force the TelnetAutomation object to bypass terminal type negotiation.
stringUserName	The username used to login to the Telnet or SSH session of the non-Windows system or device. For security reasons, you can encrypt the username into a file and then set the stringUserName as the name of the file prefixed by "file:".

You can create custom scripts or Virtual Agents to monitor Linux and UNIX systems with the eXc Software CLI-based COM objects by following a basic pattern:

- Connect and login to the host
- Execute a command on the remote host and grab the results
- Process the results
- Create WMI event to be processed by MOM 2005

Shortcuts…

Tweaking the Virtual Agent with Your Own Code

Within the __VirtualAgentFactory.js script you can modify which business logic scripts (i.e., Virtual Agents) get associated with the WMI host object. By editing __VirtualAgentFactory.js and __VirtualAgentJobs.wsf, you can implement your custom Virtual Agent code and make calls using CLI or SNMP protocols.

In the WSF file, you can add additional scripts to the ALL job to be run with all the other scripts at the set interval. For example, if you had a script to monitor I/O rate of a particular fiber-channel HBA named FCHBAUtilization.js, you would add the following in the job with the ID of ALL:

```
<script language="JScript" src="../../FCHBAUtilization.js">
</script>
```

Each time the Virtual Agent runs the job ALL, the FCHBAUtilization script will run along with the CPU and Disk utilization scripts, among others.

On the other hand, if you have created your own complete SNMP or CLI-based Virtual Agent and want to perform specific processing outside of the default processing, call your custom Virtual Agent from inside __VirtualAgentFactory.js.

For more detailed information regarding customizing your eXc Software solution, go to www.excsoftware.com.

Although the APIs provide a wide range of things you can do programmatically to handle just about every automatable condition on your Linux and UNIX servers, the pattern stated earlier will be used in just about all your custom scripts. The following code demonstrates some of the basic routines that you will need to perform.

The very first step is to instantiate the TelnetAutomation object so you can call the methods needed to communicate with the remote managed system. Here is an example of how to instantiate the TelnetAutomation object:

```
var g_objTelnetAutomation = new
ActiveXObject("NamespaceTelnetAutomation.ClassTelnetAutomation");
var g_objWMI = null;
```

Once you have instantiated the object, you are ready to start calling its methods, such as Autostart. Remember that Autostart is an efficient way to populate the necessary properties with the values for the host (read from the __Hosts.csv file), connect, and login.

```
var l_objArgs = WScript.Arguments;
g_objTelnetAutomation.AutoStart(l_objArgs(0), WScript.FullName, true, true);
g_objWMIInstance = GetObject("winmgmts://./root/cimv2:" +
   eXc_nonWindows_OperatingSystem.Name='" + l_objArguments(0) + "'");
```

Once you have successfully connected and logged in to the host (via AutoStart), you will be able to start passing commands and capturing the results. The following is an example of using the TelnetAutomation object to invoke a command and grab the results.

```
var l_ulongCommandLine1 = g_objTelnetAutomation.key("df -h");
var l_stringData1 = g_objTelnetAutomation.getData(l_ulongCommandLine1);
```

With the command's output in a standard string variable, you can parse or extract the data and apply business logic to process the results. The end goal is to create WMI events that will get forwarded to MOM 2005 so they can be processed by event rules that you have created in your custom management packs.

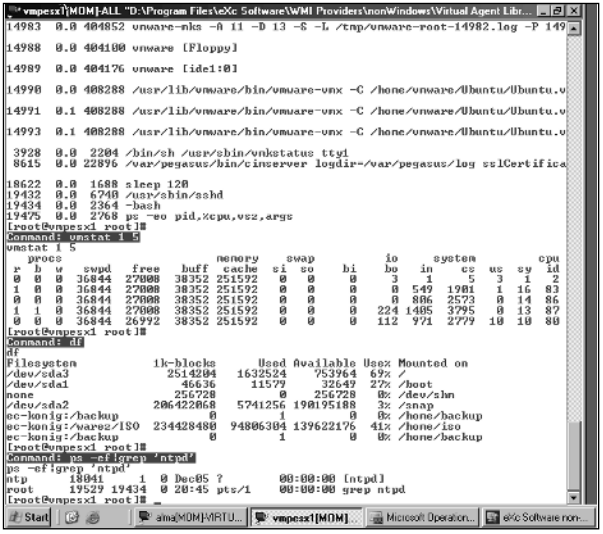
```
var l_objArgs = WScript.Arguments;
var l_Date  = new Date();

l_strAction = "ADD";
l_strUUID = "0";
l_strSeverity = "3";
l_strSource =l_objArgs(0);
l_strGeneratedBy = "eXc Virtual Agent " + WScript.ScriptFullName;
l_strTarget_Type = "nonWindows";
l_strStart_Date_Time = l_Date.toUTCString();
l_strState = "NEW";
l_strAssigned_To = "UNIX Administrators";
l_strLast_Update = "";
l_strETA = "";
l_strDescr = l_stringData1;
l_strNotes = "";
g_objWMI.SendEvent(l_strAction, l_strUUID, l_strSev, l_strSrc,
      l_strGeneratedBy, l_strTarget_Type, l_strStart_Date_Time, l_strState,
      l_strAssigned_To, l_strLast_Update, l_strETA, l_strDescr, l_strNotes);
```

Figure 10.17 shows the CLI interaction with a Linux host. The Virtual Agent calls the business logic routines in intervals previously established, and the various business logic scripts run inside one or more command shell windows. In this particular example, the **vmstat 1 5** command is being run to gather performance counter

statistics, **df** is run to gather disk usage statistics, and **ps –ef | grep 'ntpd'** is being run to determine if a critical process is currently running or not. The output, or results, is being stored in string variables for additional processing later.

Figure 10.17 CLI Commands Being Run against Linux Host



The eXc Software non-Windows Event Provider and base framework delivers a highly extensible way to monitor your Linux and UNIX systems. Using a smart collection of COM objects that support both SNMP and CLI-based interaction with non-Windows systems, you can easily provide advanced management and integration with MOM 2005.

Some Independent Advice

If you are planning on establishing a framework for managing your non-Windows operating systems, you can get an even higher return on your investment by managing your hardware and applications, even for Windows systems.

eXc Software offers Virtual Agents for popular hardware management platforms, such as Dell Open Manage, HP Insight Manager, and IBM Director. You can also monitor IBM eServer BladeCenters directly through the management module components of the BladeCenter chassis. eXc Software can also manage popular applications such as BEA Weblogic, IBM Websphere, Oracle, Lotus Domino, Blackberry Enterprise Server, and the Citrix product line, among many others.

Finally complete your management portfolio for MOM with Virtual Agents for storage arrays, such as those from EMC, Hitachi, and HP StorageWorks as well as devices from McData, QLogic, and Brocade.

Of course, eXc's extensible Virtual Agent architecture allows you to create Virtual Agents to manage just about anything you have in your infrastructure that supports Telnet/SSH with a little custom development.

Agent-Based Management of Linux and UNIX Servers

Another method to manage non-Windows systems is to use an alternate network management system that can feed data into MOM. These types of network management systems, or NMS, employ agents that reside on each managed system to provide advanced data collection and perform responsive actions on the host systems. In this section, we will take a look at an NMS that is dependent on MOM for data storage and further intelligence in its management strategy.

The Jalasoft Xian 2005 Network Manager Server is a comprehensive systems management solution set designed to extend the knowledge-based monitoring and management capabilities of Microsoft Operations Manager to the other critical components of your computing infrastructure. Although this NMS can be used to manage many different types of systems, network devices, and other infrastructure components, we will be focusing on its ability to manage Linux and UNIX systems and how it integrates with MOM 2005.

Overview of Xian 2005 Network Manager

NMS solutions like the Xian 2005 Network Manager are not just MOM management packs or add-ons. The unique combination of MOM with Xian allows you to manage your non-Windows infrastructure components from the MOM Management Console. Xian is a complete management system that takes advantage of the Microsoft Connector Framework (MCF) to communicate with and provide feedback to MOM 2005.

Xian 2005 Network Manager is comprised of several components that can either be colocated on a single server, such as a MOM 2005 management server, or distributed across various systems to increased scalability and performance. Those components are:

- **Xian Network Manager Server (NMS)** The Xian Network Manager Server is a Windows service that can monitor systems using the SNMP protocol or using the Xian Agent. SNMP access is provided and will support every derivative of the Linux and UNIX operating system base; however, agents are currently available only for Solaris and Linux distributions that support RPM packages. For each supported device type, a specific Xian plug-in, also referred to as a Smart Management Pack, is required. For example, to monitor a Solaris server, the Xian plug-in for Solaris is required. These plug-ins include a set of rules specifically designed to monitor the network device.
- **Xian Database** The Xian Database stores all persistent information required by the application, that is, information related to plug-ins, rule templates, monitored devices, active rules, alerts, counters and more.
- **Xian Data Server** The Xian Data Server is a Windows service that may be installed on a computer with all other Xian components, or on a different computer as needed. It is used to provide read/write access to the Xian Database requested by the Xian Network Manager Server, Xian Network Scan Server, Xian Web Service, and the Xian Console.
- **Xian Connector for MOM 2005** The Xian Connector for Microsoft Operations Manager 2005 is a Windows service created to allow the migration of information about monitored devices from the Xian Data Server to the MOM 2005 Connector Framework. Data that is migrated includes the alerts and performance data generated in Xian rules.
- **Xian Network Scan Server (NSS)** The Xian Network Scan Server (NSS) may be installed on a computer with all other Xian components, or on a different computer as needed, and usually no more than one instance of this component is required for most environments.
- **Xian Web Service** The Xian Web Service provides connection between a Xian Data Server and one or more Jalasoft Xian Consoles using HTTP protocol, default port 80. It exposes a standards-based mechanism that provides connectivity between the Xian Console (web service consumer) and the Xian Data Server. No credential is required to access to this description file.
- **Jalasoft Smart Management Packs (SMP)** The Jalasoft Smart Management Packs (SMPs) are provided as AKM files in the Xian Network Manager distribution folder and must be installed before any other Xian component. Each SMP is individually licensed as are the devices managed by the SMP.

- **Xian License Manager** The Xian License Manager allows the user to add all required licenses to be used.
- **Xian Console** The Xian Console serves as the heart of the Network Manager. The Xian Console is a fully locatable user interface used to manage all rules being executed by the Xian Network Manager Server, systems being monitored, systems found with the Xian Network Scan Server, policy templates, licenses, and more.

All information generated by Xian active rules about monitored systems, its alerts, and performance data are sent to the Xian Connector for Microsoft Operations Manager 2005. The Xian Connector sends that information to the Microsoft Connector Framework (MFC 2005) and to the Data Access Server (DAS), then finally the information is available in the MOM Operator Console through the Jalasoft's SMPs. The Xian Console relies on the Xian Data Server to provide access to data in the Xian Database.

Several Xian Consoles may be connected to a single Xian Data Service using the TCP protocol, default port 8181, or to a single Xian Web Service using the HTTP protocol, default port 80. When the Xian Console is using the HTTP protocol, it becomes a *consumer of the web service* provided by the Xian Web Service component. The Xian Console is used to easily manage the following elements inside the Xian environment:

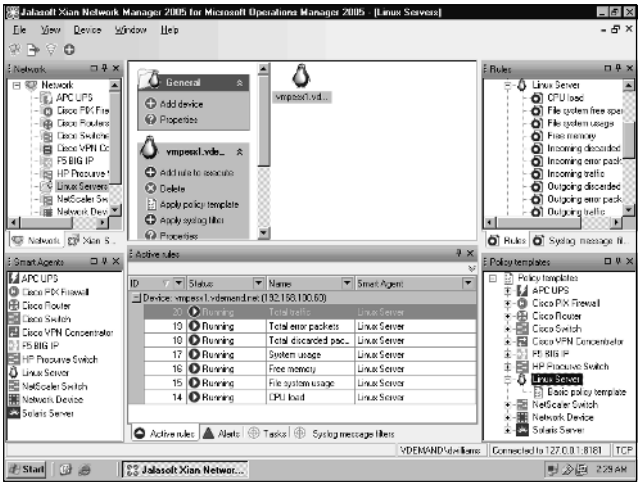
- Devices
- Active Rules
- Policy Templates
- Alerts
- Licenses

Figure 10.18 shows a sample of Xian Network Manager console. As shown, the Xian NMS is capable of monitoring and managing a wide variety of resources. For our purposes, though, we will be focusing on the Smart Agents, rules, and policy templates for Linux and Solaris.

Single Machine versus Advanced Installation

During the installation process, you will be prompted to select between two installation types. Once is a single-machine installation, where all the Xian server-side components will be installed on a single server. The other is an advanced installation, where you can choose more advanced setup options, including the distribution of the Xian components across various machines.

Figure 10.18 Xian Console with Focus on Linux Management



Before you can choose which installation type is right for you and your environment, you will need to understand the limitations of Xian Network Manager. Those limitations are outlined in Table 10.5.

Table 10.5 Sizing Limitations for Xian Network Manager

Xian Component	Limitation
Xian Network Manager Server (NMS)	A single installation without any other components installed on the same server can monitor up to 50 devices/systems. Installed with another component, the NMS should be calculated to support only 30 devices/systems.
Xian Data Server (DS)	A single installation without any other components, the DS can support up to 5 NMSes. This means that it can support at most 250 devices/systems. To scale beyond 5 NMSes, you will need to deploy additional DSes.
Xian Network Scan Server (NSS)	This component requires a high amount of network traffic to discover manageable resources. As a result, if it is installed on the same server as any other component, it may reduce that component's total capacity, as is the case with the Xian NMS and DS.

Continued

Table 10.5 Sizing Limitations for Xian Network Manager

Xian Component	Limitation
Xian Web Service	This component may be installed on another system. Since it requires IIS 6.0 with ASP.NET enabled, there may be a conflict with your organization's security policy and running some of the other Xian components on the same servers as IIS.

Select the Advanced setup type to:

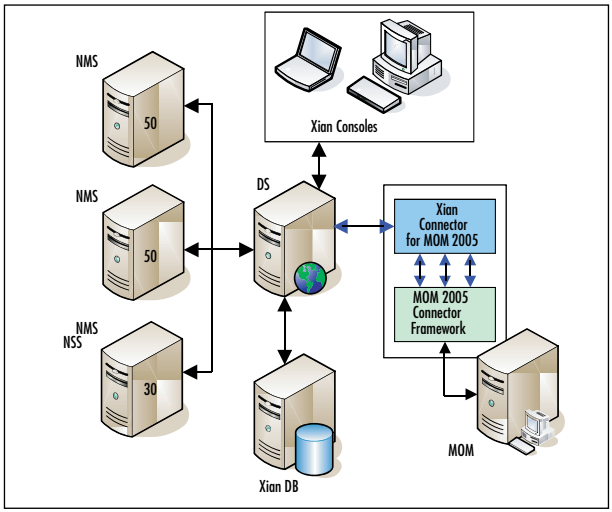
- Install one or more Xian components in the local machine
- Customize the configuration of the components to be installed.

There are some factors that you must consider, such as component placement, compatibility, and security, when planning for your Xian Network Manager installation; however, the product is robust and capable of sustaining a high load. This setup type is intended for fine tuning and for distributed deployments of Xian components in medium and large environments. Distributed environments provide Xian with a high scalability in its monitoring capabilities, every Xian Network Manager Server (NMS) installed in a dedicated machine is able to monitor up to 50 network devices; the Xian Data Server installed in a dedicated machine is able to support up to 5 NMSes.

However, you will have to decide if you are going to install all the components, except for the database, on the same server (easiest and most simple deployment) or if you're going to distribute the components with the advanced setup. Figure 10.19 shows an example of a scalable and common distributed installation. Notice that this configuration is capable of supporting 130 managed systems. To support additional systems, you would add other Xian NMSes and possibly another DS, if needed.

Select the Single Machine setup type to install all Xian components on a local machine, and to optionally install the Xian database on a different computer. This setup type is intended for small environments or testing purposes. The Single Machine setup type installation includes the Xian Network Scan feature, which scans a network segment for supported network devices and adds them to the Xian environment. If the user selects the Xian Network Scan feature to be used in the installation process, the installer will ask the user for a network segment, a list of valid SNMP community strings, and a valid basic license.

Figure 10.19 Example of a Scalable and Common Distributed Installation



Some Independent Advice

Special attention always should be paid to licensing when deploying any software product. In the case of Xian Network Manager, there are many moving pieces, all individually licensed. To make sure that you understand the cost implications of your design, let's consider a sample deployment of Xian NMS that will manage 150 Linux servers, 50 Solaris servers, 100 Cisco switches, routers, and firewalls, and 10 F5 Big IP Layer 7 switches.

In this example, we have determined that we can share the same SQL Server 2000 installation that hosts our MOM 2005 databases. One of our Xian NMS nodes will also function as a Xian NSS, supporting 50 managed devices. The remaining NMS nodes are standalone, each supporting 100 managed devices. The Xian DS will be a standalone node. Finally, the Xian Connector and Web Service will be colocated on our MOM management server with the DAS role. This configuration is similar to the one shown in Figure 10.19, with additional NMS nodes to support the number of devices and systems to be monitored.

For our scenario, we will need the following licenses:

- One Xian Network Manager Bundle (MOM 2005 Edition) – This includes the licenses for a single Xian NMS (with a monitoring capacity of up to 50 devices), NSS, DS (with a capacity of 5 NMS connections), and a Xian Connector. This bundle is a requirement for any other license.

- Three additional Xian NMS licenses
- 150 Xian Linux Agents (MOM 2005 Edition)
- 50 Xian Solaris Agents (MOM 2005 Edition)
- One Smart Management Pack Bundle for Cisco Devices
- One Smart Management Pack for F5 Big IP
- One Smart Management Pack for Linux
- One Smart Management Pack for Solaris
- 100 Device Licenses for Cisco Devices – The prices varies depending on device type (switch, router, firewall, etc.)
- 10 Device Licenses for F5 Big IP

The choice of a single-machine install or an advanced, distributed install is a matter of scale. If you will be monitoring only a small number of systems, you will need only one system to house the application. Once you've outgrown that first installation, you only need to add additional dedicated NMS nodes. However, if you know that your organization has a hundred or more Linux or UNIX systems to manage, you should choose a more distributed install, as shown in Figure 10.19.

Managing a Linux/UNIX Systems with an Agent-based Network Manager

In the following section, we will walk through the installation steps for a new deployment of the Jalasoft Xian Network Manager. We will configure Xian to monitor a Red Hat system with the Smart Management Pack (SMP) for Linux. These steps should quickly get you managing your Red Hat systems with MOM 2005.

We will review the steps to install Xian Network Manager on a single machine as well as a more distributed deployment. Before beginning the installation of any eXc Software components, all software requirements must be satisfied. Table 10.6 shows what items need to be installed as a prerequisite for each component.

Table 10.6 Software Requirements for Jalasoft Xian Network Manager

Windows Server Version	Requirement
Xian Network Manager Server	Microsoft Windows 2000 SP4, Windows 2003 Microsoft .NET Framework 1.1 or later MDAC 2.6 or later SNMP connectivity to all devices to be monitored

Continued

Table 10.6 continued Software Requirements for Jalasoft Xian Network Manager

Windows Server Version	Requirement
	Connectivity via TCP port 8181 to a Xian Data Server
Xian Database	Microsoft Windows 2000 SP4, Windows 2003 Microsoft SQL Server 2000 SP3 or later Administrative privileges to create databases
Xian Data Server	Microsoft Windows 2000 SP4, Windows 2003 Microsoft .NET Framework 1.1 or later MDAC 2.8 or later Connectivity to the Xian Database Connectivity via TCP port 9595 to a Xian Connector
Xian Connector for MOM 2005	Microsoft Windows 2000 SP4, Windows 2003 Microsoft .NET Framework 1.1 or later MDAC 2.8 or later Connectivity via TCP port 8181 to a Xian Database MOM 2005 Framework Connector MOM 2005 Data Access Server (DAS)
Xian Network Scan Server	Microsoft Windows 2000 SP4, Windows 2003 SNMP connectivity to all devices to be monitored Microsoft .NET Framework 1.1 or later MDAC 2.6 or later Connectivity via TCP 8181 to Xian Data Server
Xian Console	Microsoft Windows 2000 SP4, Windows 2003 Microsoft .NET Framework 1.1 or later MDAC 2.6 or later Connectivity via TCP port 8181 to a Xian Data Server

Continued

Table 10.6 continued Software Requirements for Jalasoft Xian Network Manager

Windows Server Version	Requirement
Xian Web Service	Microsoft XP, 2000, or 2003 IIS Web Server Microsoft .NET Framework 1.1 or higher MDAC 2.6 or later Connectivity via TCP port 8181 to a Xian Data Server
Xian Reports for MOM 2005	Microsoft Windows 2000 SP4, Windows 2003 Microsoft SQL Server Reporting Services MOM 2005 Reporting Admin privileges to SystemCenterReporting DB

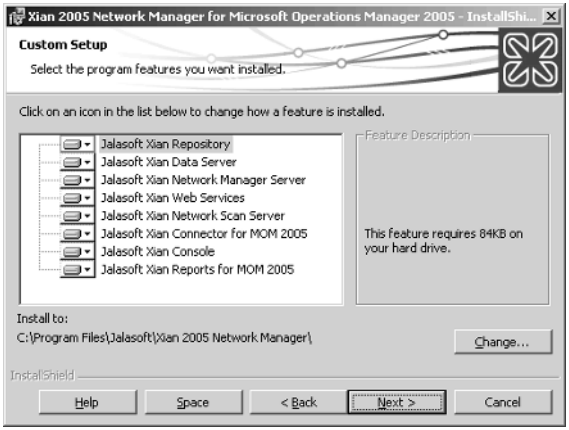
Once the prerequisites are installed, you can perform the installation steps. You can download the latest version of the Xian Network Manager from www.jalasoft.com. At the time of publishing this book, the latest version was Xian 2005 Network Manager SP2.

Installation of Xian Network Manager

After you have downloaded the installation package and run the installer, you will be presented with the option to pick the setup type – either Single Machine or Advanced. This walk-through assumes that you will by choosing the Advanced setup option but installing all components on the same management system. The assumption is also being made that this system will also be a MOM 2005 Management Server with the DAS role. If you are not planning on distributing the Xian Network Manager components, you can still follow these steps for a distributed installation. Some components may not be available to install if the target machine does not fulfill the installation requirements. To install Xian Network Manager, use the following steps:

1. The first step in the wizard is to pick your components. Since we are installing all the components, we will leave them all selected (see Figure 10.20). However, if you want to distribute the components, you should leave only the components to be installed selected and deselect the others.
2. Click **Next**.

Figure 10.20 Xian 2005 Network Manager Customer Setup



3. On the Xian database information page, enter the server name (and instance, if relevant) and the database name to be created for Network Manager. Also, select the authentication mechanism. If you choose **Use NT Authentication**, the account used to run the Xian Network Manager Service will need to have dbo access to the database. If you choose **Use SQL Server Authentication**, you will have to specify a SQL login that has database creator rights on the SQL Server.
4. Click **Next**.
5. Configure the Xian Data Server by setting the **Xian Data Server Port** (8181 is the default value). This port will listen for requests from the Xian Console, Network Manager Servers, Network Scan Servers, Web Services, and the Xian Connector.
6. Select **Connect to repository using current configuration** (see Figure 10.21). If you are installing a standalone data server, you would configure connectivity to another existing repository.
7. Click **Next**.
8. Configure the NMS component by selecting **Connect to local Data Server** (see Figure 10.22). If your data server is on another system, be sure to configure connectivity to it by entering the IP address as well as the port the data server is configured to listen on.

Figure 10.21 Xian Data Server Configuration

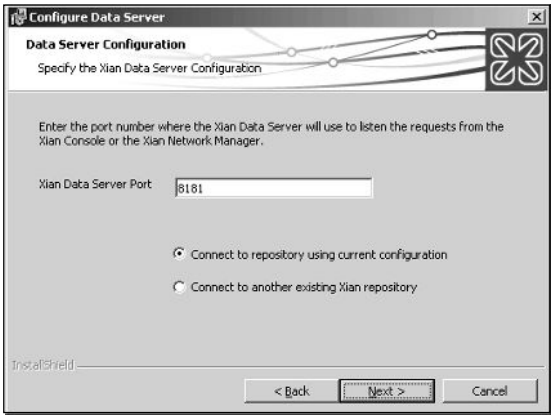
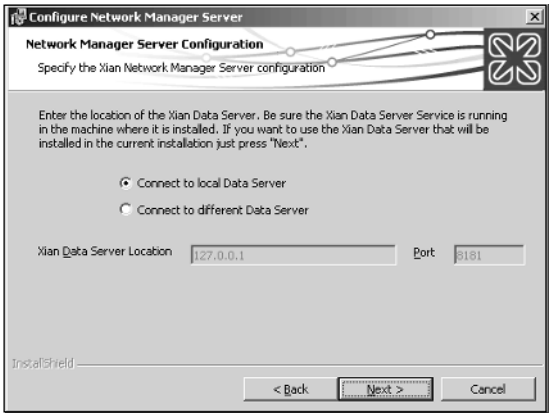


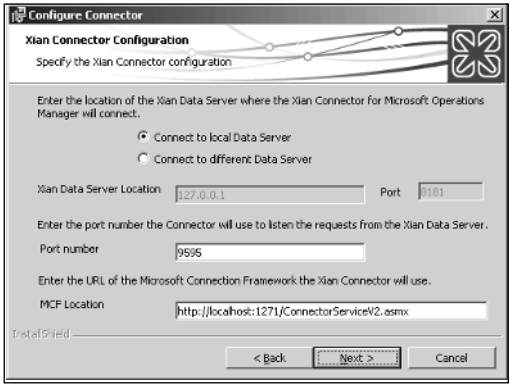
Figure 10.22 Configure Network Manager Server (NMS)



9. Click **Next**.
10. Configure the Web Service by choosing **Connect to local Data Server**.
11. Click **Next**.
12. Configure the NSS component by selecting **Connect to local Data Server**.
13. Click **Next**.
14. Configure the Connector for MOM 2005 by selecting **Connect to local Data Server**.
15. Enter the port number the Connector will use to listen for requests from the Xian Data Server. By default, this port number 9595.

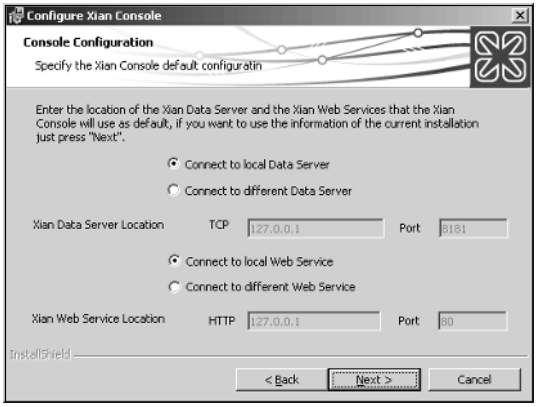
16. Enter the URL of the Microsoft Connector Framework hosted on a MOM 2005 DAS. If the DAS is installed locally on the server, the default URL is *http://localhost:1271/ConnectorServiceV2.asmx* for the **MCF Location** (see Figure 10.23).

Figure 10.23 Configure Xian Connector for MOM 2005



17. Click **Next**.
18. Configure the System Center Reporting database account, including the authentication method, server name and instance, database name, and username and password if SQL Server Authentication is selected.
19. Click **Next**.
20. Configure the Xian Console by selecting **Connect to local Data Server** and **Connect to local Web Service**. If those components are hosted on another server, enter the appropriate IP address for **TCP** or **HTTP** as well as the **Port** that the component is listening on (see Figure 10.24).

Figure 10.24 Configure Xian Console



21. Click **Next**.
22. Enter the **Domain\User Name** and **Password** for the service account used to run the Xian services. The username for the services must have administrator access rights on the management server. It must also have *Log On As A Service* privileges.
23. Click **Next**.
24. Click **Install**.
25. Click **Finish**.

Best Practices According to Microsoft

- **Plan...plan...plan**. Be sure to put in enough time planning up front to avoid any complications later on. It will delay your deployment timeline to have to rearchitect on the fly, or you may not be able to exploit the full potential of the product if your solution is undersized.
- **Make the most out of each license you purchase**. When planning, factor in the type of hardware that you will be running each component on. Although we discussed 50 as the number of systems that a Xian Network Manager Server can support, you may be able to support much more depending on the type of processors, quantity of processors, and the amount of memory your NMS has. For example, a 4-way dual-core AMD Opteron server with 4 GB of RAM will be able to monitor more systems that a 2-way Intel XEON with 1GB of RAM and Hyper-threading disabled. However, the maximum monitoring capacity for a single NMS is 200 systems/devices.
- **Share resources**. Considering today's hardware, colocating systems management components is possible without causing them to fight for resources. Be sure to install components (some if not all) on one of your MOM 2005 Management Servers to get the most utilization from your existing hardware investment.
- **Never install the database component with the other Xian components**. Although it's possible, do not install the production Xian database on the same server as any other Xian component. Doing so will significantly reduce the capacity of that component. Consider placing the Xian database on the same server as your OnePoint and/or your SystemCenterReporting database if appropriately sized.

Configuration of Xian Network Manager

Now that the Xian 2005 Network Manager SP2 components have been completely installed, you should import the Smart Management Packs (SMPs) and Reports into your MOM 2005 configuration. SMPs provide the intelligence to organize, process, and analyze the information gathered by Xian into the views, computer groups, and reporting capabilities of MOM. SMPs are device-aware and tailored to the monitoring and management requirements of each type of device and vendor product. Views provided for each supported device include:

- Alerts and notifications
- Performance.
- Performance data
- Computer
- Computer attributes
- Topology
- State

Xian 2005 Network Manager comes with its own SMP to manage the health and performance of the Jalasoft Xian Network Manager environment. SMPs also provide a large set of reports created to incorporate historical and trend analysis capabilities, based on performance data collected by the most relevant Xian monitoring rules.

To install the Jalasoft Smart Management Packs and reports using the Microsoft Operations Manager Administrator Console, execute the following steps:

1. In the Navigation pane, click **Management Packs**.
2. In the Detail pane, click **Import/Export Management Packs** to open the Management Pack Import/Export Wizard.
3. Follow the instructions in the Management Pack Import/Export Wizard.
4. When asked, select all Smart Management Packs and reports to import.

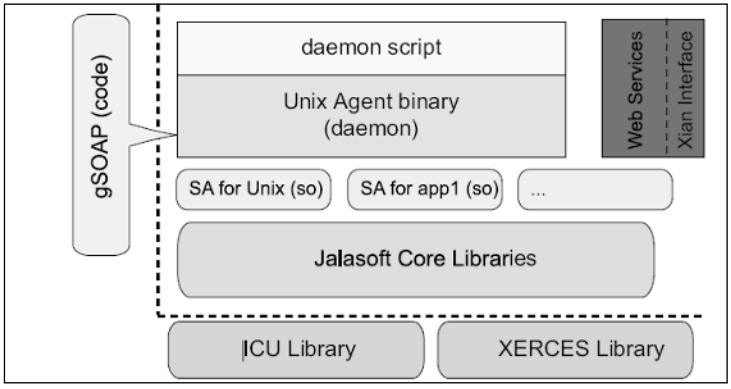
Installing the Xian UNIX Agent for Linux and Solaris

Although Xian Network Manager can monitor and manage devices and systems with the SNMP protocol, effective management for Linux and Solaris systems is best achieved using the Xian Agent. The Xian UNIX Agent is able to load various different shared objects (so) at run-time and publish information about the status of the server or applications via Web Services, as shown in Figure 10.25.

The basic shared object is the UNIX so. This so, depending on the OS version, will have different names. For example for the Linux OS, the shared object is *libjsrhu.so*. The UNIX so must be present at all times; other sos may be loaded at the same time, later, or not at all.

Each loaded so will allow the Xian UNIX Agent to publish, via Web services, information about the particular OS or Application it was design to monitor. The corresponding plug-in in Xian will be able to request the Xian UNIX Agent discovery information or the status of any discovered node in that server.

Figure 10.25 Xian UNIX Agent for Linux



The Xian UNIX Agent for Linux comes as an RPF file, *XianServer-x.x.x.x.-n.rpm*, where *x* refers to the build number and *n* is the version. To install the agent, you need to be logged in as root and run the following command: **rpm –ivh XianServer-x.x.x.x.-n.rpm**. For Solaris systems, the UNIX Agent for Solaris comes as a TAR file, *XianServer-x.x.x.x-n.tar.gz*.

After the installation, you have the option of fine tuning the Xian Server configuration file, *xianserver.conf*. A sample of the configuration file is as follows:

```
# Log settings
%loglevel 10
%logname /var/log/xianserver
%logsize 8388608
# Web Services settings
%port 8182
%queue 100
#Enter Server information below (as you wish to appear in MOM 2005)
%Contact MIS Department
%Location Corporate Data Center - Rack 2B
```

Shortcuts…

Avoid Overmonitoring Your Systems

Monitoring your critical infrastructure components is an important component of managing an enterprise infrastructure. However, it is possible to over-monitor your servers. Excessive monitoring is usually the result of too many monitoring processes running on your systems, consuming valuable resources that your applications need. Many times, the various agents that are installed on your servers are collecting the same data (in particular performance counters and events) and possibly each attempting to remedy the same condition or issue. Among the various agents that may already exist on your Linux or UNIX servers, you may be running the following:

- HP Insight Agents (Foundation Agent, NIC Agent, and Storage Agent)
- IBM Director Agent
- Dell OpenManage Agents
- IBM Tivoli Agent
- BMC Patrol Agent for Linux or UNIX

If you already have one or more of these processes running, you should consider using an agentless approach to get performance and event data into MOM. Both Xian NMS and eXc Software have the ability to use SNMP to manage *NIX servers without relying on an agent process on the managed host.

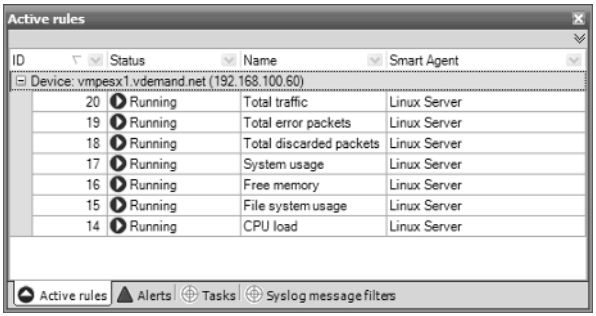
Xian Rules and Policy Management

Xian rules are the basic monitoring element used to monitor known devices or objects included in those devices. These rules monitor devices or their included objects, requesting information about internal counters or status of the monitored device. Every Xian rule may generate alerts, which are sent to the MOM 2005 environment as MOM alerts. Monitoring rules may generate performance counters, which provide information about the monitored device over time; these counters are sent to the MOM 2005 environment as MOM performance data.

Out of the box, the Linux agent monitors network interfaces focusing on errors and discarded packets, memory, file systems, and CPU load. The active rules are based on templates that ship with the product. You can add or remove rules as well

as create new rules from your own custom templates. Figure 10.26 lists the rules that are active after install for Linux systems.

Figure 10.26 Active Rules for Linux



Jalasoft Xian Network Manager provides an easy-to-use Policy Template Management solution expressly designed to deploy predefined sets of monitoring rules into the Xian environment with almost no effort.

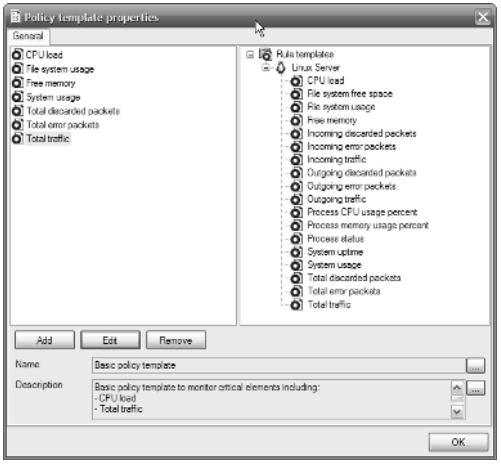
Policy templates are preconfigured groups of rules designed to easily apply a large group of rules to one or more supported devices and start to monitor them immediately. Within each policy template, rules are grouped together and alert thresholds defined. Those alerts are forwarded onto MOM 2005 by the Xian Connector. Xian 2005 Network Manager provides basic policy templates for every provided plug-in, custom policy templates may be created to satisfy user monitoring needs. Both, basic, and custom policy templates may be applied to devices located by network scan tasks automatically.

To create your own template, follow these basic steps:

1. In the Policy Template window, right-click the Smart Agent to which the policy will apply.
2. Next to **Name**, click the **[…]** button to change the name of the policy template.
3. Next to **Description**, click the **[…]** button to change the description of the policy template.
4. On the right pane you will find all the rules available from the Smart Agent. To add a rule to the policy template, click **Add** to start the Rules configuration wizard.
5. Highlight the rule you want to add and click **Next**.
6. Check **Alert when value is over threshold** and set the appropriate threshold for the monitored rule. Click **Next**.

7. Configure the severity for the alert notification forwarded to MOM 2005. Click **Next**.
8. Establish the interval that the Smart Agent will poll for data. Click **Next**.
9. Check **Collect performance data on each rule execution** to enable performance data storage in MOM. If this is not checked, the performance data for the specific counter will be used only to evaluate alerts and not retained.
10. Click **Finish**.
11. Repeat steps 1 through 10 for each additional rule to be added to the policy (see Figure 10.27).
12. Click **OK** to save the policy template.

Figure 10.27 Policy Template Properties



Once defined, the group of rules defined in the policy can be applied to any particular Linux or Solaris server or groups of servers. Data collection immediately begins as performance data (if enabled) and alerts are forwarded to MOM and available for your review in the MOM 2005 Administrator Console.

Although not as extensible as eXc Software's agentless solution, the Xian Network Manager offers robust monitoring of Linux and UNIX systems in an easy-to-manage package.

Summary

Your Linux and UNIX systems can now take advantage of the advanced manageability and reporting capabilities that Microsoft Operations Manager 2005 already provides to Windows Server System technologies. Among the points covered in this chapter, we discuss the following topics:

- Design an agentless solution to monitor and manage Linux and UNIX systems
- Install the eXc Software WMI non-Windows Event Provider and base framework
- Install and configure eXc Software Virtual Agents
- Customize SNMP and CLI-based Virtual Agents
- Design an agent-based solution to monitor and manage Linux and UNIX systems
- Install the Jalasoft Xian 2005 Network Manager
- Install the Xian UNIX Agent for Linux and Solaris
- Configure rules and policy templates to manage your Linux and Solaris servers.

Microsoft Operations Manager 2005 can be used to manage more than just Windows Server systems. Thanks to solutions from third-party vendors, it is possible to develop and deploy advanced management packs with rules to handle events and alerts. Depending on your management strategy, you can employ both agentless and agent-based technologies to interact with and gather data from your Linux and UNIX systems.

Agentless solutions are growing in popularity and have changed the management paradigm that organizations use to monitor and control their critical infrastructure resources. They have the benefit of:

- Rapid deployment
- Simple architecture
- Intelligent COM objects that integrate with WMI
- Support for both SNMP and CLI protocols

In comparison, agent-based solutions follow the traditional management model consisting of server components that communicate with lightweight agents deployed on each management node. These solutions are often:

- Very scalable
- Designed specifically for the operating system being managed
- Facilitate complex data collection options and responses

Solutions Fast Track

Agentless Management of Linux and UNIX Servers

- ☑ eXc Software's solution uses a WMI non-Windows Event Provider that facilitates the collection of performance and event data into MOM 2005.
- ☑ Virtual Agents are a combination of scripts and jobs that are used to set up and invoke the management routines that interact with Linux and UNIX systems.
- ☑ eXc Software Virtual Agents are configured using the eXc Software Configuration Utility/GUI. With this tool, you can configure the hosts monitored by the Virtual Agent, processes to be monitored, performance thresholds, syslog settings, and the Virtual Agent job settings.
- ☑ eXc Software's base framework provides an extensible platform to develop custom solutions using both SNMP and CLI-based protocols.
- ☑ The SNMP COM objects can be used to perform catch or generate SNMP traps as well as perform standard GET and SET commands against any SNMP-enabled system. The CLI COM object, TelnetAutomation, can be used to connect to managed hosts via Telnet or SSH, run command, and record the results or output from the commands.

Agent-Based Management of Linux and Solaris Servers

- ☑ Jalasoft's Xian 2005 Network Manager Server (NMS) that is comprised of multiple components that can scale to support any size infrastructure.
- ☑ Xian 2005 supports the Red Hat and SuSE Linux distributions and the Sun Solaris operating system.
- ☑ The Xian NMS uses the Microsoft Connector Framework (MCF) to integrate with MOM 2005.

- ☑ Although not as extensible as eXc's solution, Xian 2005 offers a UNIX Agent for both Linux and Solaris that tightly integrates the agent's functionality into the host operating system.
- ☑ Jalasoft's Smart Management Packs extend MOM 2005's capabilities to monitor Linux and Solaris servers. These management packs contain computer groups and processing rules, with filters, performance counters, alerts, a ready-to-use knowledge base for monitoring and managing the supporting operating systems.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: My organization uses several Linux distributions that are not listed on eXc Software's site. How can I take advantage of eXc's management framework?

A: There are too many Linux distributions to have customized Virtual Agents for each one. However, all Virtual Agents are the same in design. You can download any Linux Virtual Agent, such as the Virtual Agent for Red Hat or SuSE, and make the necessary changes to scripts and configuration files to make it work on your particular distribution(s).

Q: What scripting languages can I use to develop my own custom Virtual Agent?

A: You can use any scripting language supported by Windows Script Host 5.6. Since WSH exposes an OCX control that allows external scripting engines to hook into the host using ActiveX, just about every major scripting language is supported. The popular choices are VBScript, JScript, Javascript, REXX, Perl, and Python. However, only VBScript and JScript are native to Microsoft's operating systems.

Q: How can I integrate the hardware monitoring provided by my server hardware manufacturer into eXc's framework?

A: eXc Software provides several Virtual Agents for most of the major servers, including HP ProLiants, Dell PowerEdge, and IBM xSeries. They take advantage of the "business logic" already integrated into the hardware-monitoring

agents. In addition, you can utilize native SNMP support and direct traps to your eXc Software management server.

Q: What happens if MOM 2005 becomes unavailable?

A: With the eXc Software solution, all functionality is wrapped in a component model that is an internal part of MOM 2005. The WMI non-Windows Event Provider and the corresponding management pack are responsible for invoking the "factory" that runs the collection and monitoring jobs. In the event that MOM 2005 is unavailable, the Virtual Agents will not automatically run their jobs. Even if you run the jobs manually, you will not be able to store any data since the MOM DAS would be offline. In contrast, Xian 2005 wraps its functionality in a management system that is external to MOM 2005. Data forwarded to MOM 2005 uses the connector framework. Xian 2005 also uses its own database separate from the MOM databases. If for any reason the MOM 2005 Connector Framework is not available, then all data received by the Xian Connector from the Xian Data Server will be cached into temporary tables named *ConnectorDeviceCache*, *ConnectorAlertCache*, and *ConnectorPerformanceDataCache* in the Xian database. After the MOM 2005 Connector Framework is available, all cached information in the Xian Connector is transferred to the MOM environment.

Q: I need to make sure that critical performance data is monitored out-of-the-box without much customization of the product. What are the components monitored by each solution?

A: Out of the box, each of the products monitors several critical components without much customization. eXc Software's Virtual Agent solution monitors and creates alerts for CPU usage per process, total CPU usage, disk utilization, syslog files, and process states. Jalasoft's SMP for Linux and Solaris monitors CPU load, system uptime, system usage, file system free space, file system usage, interface traffic, syslogs, and free memory.

Q: What reports do the management packs for each product provide?

A: eXc Software provides reporting of the eXc solution including alert and event analysis as well as performance reports reflecting CPU and disk utilization. Xian 2005 SMPs provide a wide range of reports, including summary and detail view of alerts, CPU load, file system, memory, interface traffic, and system usage.

Chapter 11

Connecting to Other Management Platforms

Solutions in this chapter:

- **Overview of the Microsoft Connector Framework**
- **MOM to HP OpenView Operations Product Connector**
- **MOM to IBM Tivoli TEC Product Connector**
- **Other Connectors from Third-Party Vendors**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

Integrating enterprise management systems (EMS) is one of the key areas where businesses have elected to initiate integration projects. Over the years, hefty investments have been made in the company's IT infrastructure and framework. Additionally, as new technology and solutions are introduced, corresponding monitoring technology is also implemented. There is a tremendous need and confirmed value to tie all these disparate systems together ensuring a company's computing infrastructure is operating at peak performance.

This chapter covers some of the common connectors that can be used to integrate MOM 2005 with other management systems.

Overview of the Microsoft Connector Framework

The core component of the integration between MOM 2005 and other enterprise management systems is the Microsoft Connector Framework (MCF). The MCF is a Web service-based framework for connecting MOM and any third-party management platform and enabling full bidirectional alert forwarding and synchronization, including alert clear-downs between management tools, providing increased management benefits to both medium and large enterprises.

The MCF is based on .NET technologies. As a result it is dependent on both IIS and the .NET Framework 1.1. The MCF makes it easier to develop custom product connectors for MOM. The MCF for MOM 2005 also offers additional APIs than those previously available with earlier versions, allowing third-party vendors to develop powerful applications that facilitate integration at a much deeper level than just alerts and events.

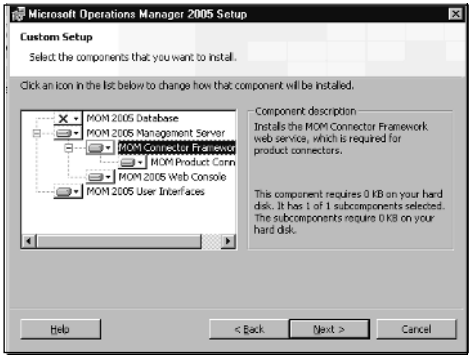
Previously available in MOM 2000 SP1 as the Microsoft Connector Feature Pack, the MCF ships with MOM 2005. MCF is a prerequisite for most of the connector products as it provides the interface for the flow of data into and out of MOM. Ensuring that it is installed and working properly is imperative to a reliable integration.

Installing MCF on a MOM 2005 Management Server

MCF is installed using the Microsoft Operations Manager 2005 Setup wizard. If you are installing a new MOM 2005 management server, the MCF will be one of the components selected during a custom setup. If you are installing the MCF on an

existing management server, you will need to launch the MOM Setup wizard and select **Modify** as your setup type to modify the existing installation and include the MCF. From the custom setup page of the wizard, be sure to set the MOM Connector Framework to **This component will be installed on local hard disk**, as shown in Figure 11.1. Since we are focusing on integrating MOM to a non-MOM EMS, installing the MOM Product Connector is optional as it will be used only to connect one MOM Configuration Group to another.

Figure 11.1 MOM Connector Framework Component Selection



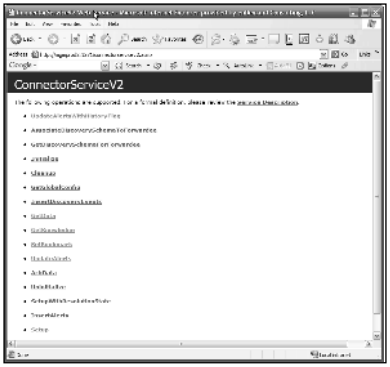
Testing MCF Readiness

To ensure that the MCF Web service is properly set up, we can load the MCF URL using Internet Explorer. From any remote system, launch Internet Explorer 6.0 or later and enter the following URL in the address bar:

```
http://[MOM-Server-name]:1271/ConnectorServiceV2.asmx
```

The result should be a listing of the available Web service operations that are available (see Figure 11.2). Each operation is listed as a hyperlink; following the link you will find a sample of a SOAP request and response for that particular operation.

Figure 11.2 Results from Browsing MCF URL



If the page shown in Figure 11.2 is not found, ensure that the MCF is installed and set up properly, and that the credentials of the account logged in on the system loading the URL is a member of the *MOM Administrators* local user group on the MOM management server.

Overview of External Third-Party Enterprise Management Systems

HP OpenView

HP OpenView is a portfolio of management solutions that helps organizations to take control of their IT and telecommunications resources. By giving them the tools to troubleshoot problems, adapt quickly to change, and keep your data secure, OpenView solutions ensure that business-critical data and services are delivered on time, all the time.

HP OpenView solutions for business, service, resource, as well as solutions specific to an industry's needs, let companies align their people, processes, and technology to contribute to an Adaptive Enterprise environment. HP's management model for the Adaptive Enterprise addresses the areas of application, business, IT service, and infrastructure management. Supporting those areas, HP OpenView also tackles governance and identity, configuration, and information lifecycle management.

IBM Tivoli

IBM Tivoli Enterprise Console provides sophisticated, automated problem diagnosis and resolution to improve system performance and reduce support costs. The latest versions focus on time to value and ease of use with out-of-the-box best practices to simplify and accelerate deployment. The auto-discovery feature allows administrators to understand the environment and process events appropriately. The Web console enhances visualization while providing remote access to events and console operations. IBM Tivoli Enterprise Console highlights:

- The real value in event management goes beyond simple filtering and provides root cause analysis and resolution. Tivoli Enterprise Console delivers this.
- The new Web console provides improved visualization as well as access from anywhere.
- Preconfigured rules provide best-practices event management out-of-the-box.

- Auto-discovery and problem diagnosis increase operator responsiveness and efficiency.
- Integrated network management extends Tivoli Enterprise Console reach and diagnosis for end-to-end management of your IT environment.
- Tivoli Enterprise Console enables comprehensive management that even accepts events from non-Tivoli products/systems.

CA Unicenter

Using an innovative, platform-independent approach, CA's Network and Systems Management solutions allow you to confidently support business initiatives with a secure, reliable, and optimized infrastructure. When the infrastructure is optimized, downtime is reduced, resource costs are controlled and the business process is more available.

These solutions support and facilitate the full range of management functions including automation, security, availability, performance, and optimization. Features such as event management, role-based visualization and security, as well as the ability to monitor locally or remotely, make Unicenter Network and Systems Management products well suited to manage both simple and complex environments.

Micromuse Netcool

The Netcool suite offers five product families that support domain-specific IT management, end-to-end consolidated operations, and business service management. Armed with industry-leading Netcool technology, organizations can collect real-time data from across the IT infrastructure, consolidate this data into a single real-time management console, analyze the data and automate responses, and inform other key individuals, systems, and processes about service-affecting IT problems. Netcool suite is comprised of the following product families:

- **Netcool/Omnibus** Real-time, end-to-end management
- **Netcool/Monitors** Trended performance, status, and service monitoring
- **Netcool/Precision** Discovery, topology, and root cause analysis
- **Netcool/Impact** Business and service impact analysis
- **Netcool/Dashboards** Real time service views, modeling, and reporting

MOM to HP OpenView Operations Product Connector

The Microsoft MOM to HP OpenView Operations Product Connector enables the integration of MOM 2005 alerts into HP OpenView Operations (HP OVO). The current MOM to HP OVO Product Connector is designed to allow any event from a MOM 2005 management server to be forwarded to OVO. Once an event is modified/resolved on the MOM 2005 server, and also has been previously forwarded to OVO server, it will also be updated/acknowledged on the OVO server.

If an event on the OVO server is acknowledged, which was generated originally from the MOM 2005 management server, the event will be resolved on the MOM server as well.

The MOM to HP OVO Product Connector runs as a service on a system that has network access to at least one MOM 2005 management server in your MOM configuration group. It may be installed on a MOM server or stand alone (see Figures 11.3 and 11.4).

Figure 11.3 MOM to HP OVO Product Connector and MOM 2005 on the Same System

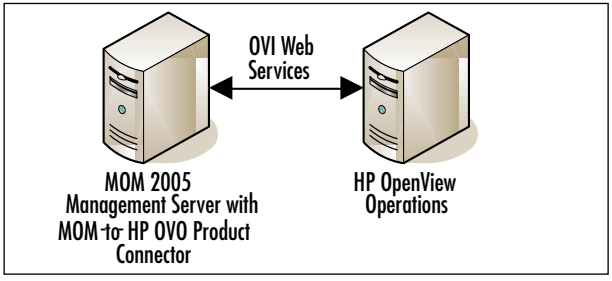
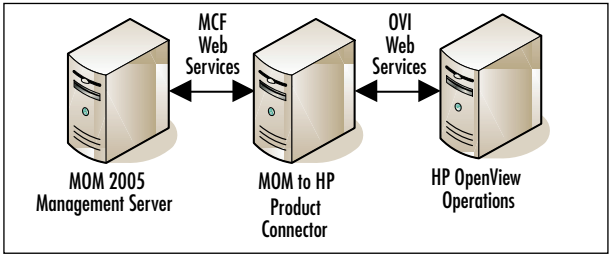


Figure 11.4 MOM to HP OVO Product Connector and MOM 2005 on Separate Systems



The MOM to HP OVO Product Connector uses custom Application and Message Groups to allow OVO to identify alarms created from MOM alerts. To be as transparent as possible, the alarms appear to come from the system that created the MOM alert, not the MOM 2005 management server. This was made possible by the integration logic between the MOM to HP OVO Product Connector and the HP OVI and the HP OV EC.

Connecting MOM to HP OpenView

The complete solution comprises several components. Outside of the MOM to HP OVO Product Connector, you will also need an HP OpenView Operations server that has the HP OpenView Interconnect installed. The installation of the MOM to HP OVO Product Connector is done in four basic steps:

1. Install the HP OVI on the HP OVO for Windows or UNIX (if not already installed).
2. Install the MOM to HPOVO Event Consumer.
3. Install the MOM to HP OVO Product Connector service.
4. Import the MOM to HP OVO Product Connector Management Pack.

Installing the HP OpenView Interconnect (OVI)

The HP OVI is the Web service-based integration point for the HP OpenView system, similar to what the MCF is to MOM. In order to install the HP OVI (latest version at the time of this writing is version 3.3), you have to meet the following system requirements.

For HP OVO for Windows (HP OVO/W):

- Windows® 2000 SP4 or later
- Microsoft .NET Framework 1.1 or later
- Windows Installer 3.0 or later
- Java Runtime Environment (JRE) 1.4.x or later
- HP OpenView Operations for Windows (OVO/W) 7.x or later
- HP OpenView Interconnect (OVI) 3.0 or later

For HP OVO for UNIX:

- HP-UX 11.xx, Solaris 8 or later, or Linux 7.1 or later
- Java Runtime Environment (JRE) 1.4.2.03 or later for HP-UX

- Java Runtime Environment (JRE) 1.4 for Solaris
- HP OpenView Operations (OVO) 7.x or later
- HP OpenView Interconnect (OVI) 3.0 or later

In addition, you must have the appropriate patches installed on HP-UX and Solaris so that the OVI pluglet licensing logic works correctly (see Table 11.1).

Table 11.1 Patches Required for HP OVI Installation

Platform	Patches Required for OVI Licensing
HP-UX 11.0	PHSS_26945, PHCO_2773
HP-UX 11.11	PHSS_22898 , PHCO_24400
Solaris 2.8	Patch-ID# 108434-14. See *http://www.sun.com/bigadmin/patches/index.html*
Solaris 2.9	Patch-ID# 111711-09. See *http://www.sun.com/bigadmin/patches/index.html*

The HP OVI can be downloaded from http://devresource.hp.com/drc/ovit/index.jsp. To install the HP OVI, complete the following steps:

1. Launch the install program. For Windows, run **OVI_33_install.exe**. For UNIX or Linux, extract the **OVI_33_install.tar** file, and run the install script.
2. Select to perform a custom installation.
3. Select both the OVO pluglets and OVOW pluglet from the **Choose OpenView Interconnect Components**.

If installing the OVI on a Windows-based HP OVO system, you can install the OVI as a service by running the following in a command prompt after running the general install:

```
"\Program Files\HP OpenView\bin\OVIService.wsf" -install <service-name>
     { -env <environment file> | {-d <deploy file> -o <output log>} }
     -e <error log>
```

Installing the MOM to HP OpenView Event Consumer (EC)

To configure the HP OVI to process events to and from MOM 2005, the MOM to HP OVO Event Consumer must be installed. To perform the installation of the HP OV EC, use the steps that follow for the appropriate operating system.

For HP OVO for Windows:

1. Run **MOM_to_HPOVOW_EC_Setup.msi** from the installation point.
2. Click **Next**.
3. Select the installation folder where you want the HP OV EC to be installed.
4. Click **Next**.
5. Confirm Installation and then click **Next** to continue.
6. A window will appear and the install process will start. After a moment the installer will pop up the **Set Service Login** screen. Enter a user that has administrator rights on the local machine to run the service. This service makes WMI calls to the HP OVO Server, so the account you enter must have Administrator rights on the local server.
7. Set fields, then click **OK**.
8. Click **Close** to complete the install.

You will now have two new services, **MOM to HP OVOW Event Consumer** and **OVI to MOM** installed and set to Automatic start.

For HP OVO for UNIX:

1. Log onto the HP OV server as **root**.
2. Run the **install.sh** from the install media.
3. Type **yes** to continue.
4. Read the End User License Agreement (EULA) and type **yes** if you agree.
5. You will be asked for a username and password to connect to the MOM to HP OVO Product Connector. You will use the same username and password when you install the Product Connector next.
6. The script will verify that all requirements have been met, and then it will install all files and start all necessary daemons for the **MOM to HP OVO Event Consumer** to run properly.

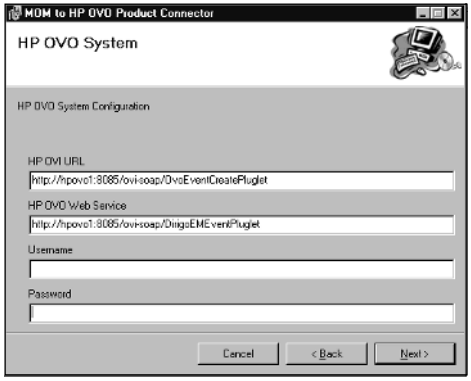
7. Once all files have been copied, verify the **momackmsg** and **OVI** daemons are running.

Installing the MOM to HP OVO Product Connector

To install the MOM to HP OVO Product Connector on the MOM 2005 management server, use the following steps:

1. Launch the install by running **MOM_to_HPOVO_PC_Setup.msi** on the MOM server if colocating MOM and the Product Connector or on standalone server.
2. Agree to the EULA
3. On the **HP OVO System Configuration** page, replace "localhost" with the DNS host name of your HP OVO system for the OVI and OVO Web Service URLs (see Figure 11.5). (You can leave "localhost" as the host name if the MOM to HP OVO Product Connector is being installed on an HP OVO for Windows server with HP OVI installed.)

Figure 11.5 HP OVO System Configuration



4. On the **Define DCAM Servers** page, enter the name of the MOM 2005 management server hosting the MCF.
5. On the **Select Installation Folder** page, enter the folder path to where you want the Product Connector installed. Be sure to select **Everyone** before clicking **Next**.
6. The **Confirm Installation** page will appear. Select **Next** to start the install.
7. The **Installing MOM to HP OVO Product Connector** window will appear. Shortly afterward a **Set Service Login** window will pop up. Enter

the DAS account used when MOM 2005 was installed. Note that this must be a domain-level account, not a local account on the MOM management server.

8. Once the installation has completed successfully, manually start the **MOM to HP OVO Product Connector** service.

If the MOM to HP OVO Product Connector was not installed on a MOM 2005 management server, the MOM to HP OVO Management Pack will need to be imported manually. Using the MOM 2005 Administrator Console, perform the following steps:

1. Launch the Import/Export Management Pack wizard to import the management pack.
2. Select to **Import Management Pack and/or Reports**.
3. During the import wizard, browse to the location of the **MOMtoHPOVOProdConn.akm** file.
4. Select to **Replace existing Management Pack** and uncheck **Backup existing Management Pack**.
5. Click **Next** to start the import.

Configuring HP OVO

After the MOM to HP OVO Product Connector has been successfully installed, you must configure the HP OVO server to properly display events and alerts of managed systems. To accomplish this, you create a managed node in HP OVO for each IP address that will be passed by MOM. The following is a walk-through of performing this task on an HP OVO/W; however, the steps are similar if your HP OVO is UNIX-based. To configure the HP OVO/W, perform the following steps:

1. On the OVO/W server start the HP OpenView Console.
2. If a login window appears, enter the name of the OVO/W server that you installed the **MOM to HP OV Event Consumer** on, then the username and password and login.
3. Once the Console is running, in the left-hand pane, expand the **Operations Manager** tree and highlight **Nodes**. Right-click it and select **Configure, Nodes**.
4. The **Configure Managed Nodes** window will appear. Expand the **Discovered Nodes**, then **Directory**, then the name of your domain in the left-hand pane.

5. Select the nodes to be managed by dragging them into the right-hand pane under **Nodes**.
6. Click **OK** to close the Configure Managed Nodes window.

Shortcuts…

Navigating HP OpenView Operations for Windows

While setting up the nodes for hosts managed by MOM, you may find that some of the steps are complicated and/or tedious. Here are some tips to make navigating HP OpenView a little more friendly.

- It's a good idea to manage the MOM server that is forwarding events to OVOW. This will help track the nodes managed by MOM as well as associate those nodes to their IP addresses easier.
- If your domain is very large you can find or add a node manually. To find or add a node, highlight the Nodes folder in the details pane and right-click.

When MOM forwards an event to OVO/W, the IP Address of the node that originally generated the event will be the source of the event in OVO/W. For OVO/W to manage it correctly you must set the Network property to be managed by the IP Address.

1. Right-click the managed node and select **Properties**.
2. Once the Properties window opens, select the **Network** tab.
3. Select **Use: IP Address** under **Server to Node Communications**.
4. Click **OK** to close the Properties window.

Now you should be ready to install the MOM-opcmsg policy. All messages forwarded from MOM to OVO/W need to be matched to an opcmsg policy. The MOM-opcmsg policy needs to be installed on the OVO/W server you installed the MOM to HP OVO Event Consumer on. To install the MOM-opcmsg policy, follow these steps:

1. Open the HP OVO Console.

2. If a login window appears, enter the name of the OVO/W server that you installed the **MOM to HP OVO Event Consumer** on, then the username and password and login.
3. Once the Console is running, in the left-hand pane, expand **Operations Manager**, then **Policy management**, then **Policy groups**, then the **Microsoft Operations Manager** tree.
4. In the details pane, highlight the **MOM-opcmsg** policy, right-click and select **All Tasks\Deploy on** from the drop-down menu.
5. The Deploy Policies window will appear. Check the box next to the Management Server you installed the **MOM to HP OVO Event Consumer** on then click **OK**.

Once the policy is pushed down to the Management Server, the connector setup and configuration will be complete. HP OpenView Operations is now configured to handle events from MOM.

MOM to IBM Tivoli TEC Product Connector

Similar to the MOM to HP OpenView Operations Product Connector, Microsoft also provides a connector for IBM's Tivoli Enterprise Console (TEC). Tivoli TEC is a very advanced, yet complicated, product and diving deep into its feature set and administration is out of scope for this chapter. However, if your organization already has an investment in Tivoli TEC and the primary enterprise management system, you should know how to connect the events and alerts from your MOM 2005 deployment into Tivoli TEC to achieve that single-point-of-view for the entire infrastructure.

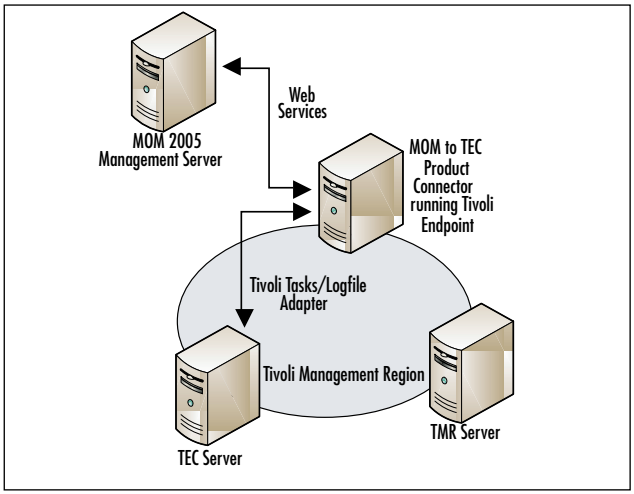
The MOM to Tivoli TEC Product Connector differs from the HP OVO connector we discussed earlier in this chapter in that it is true two-way integration. Not only can you send events and alerts from MOM to Tivoli TEC, but you can also integrate TEC events into MOM.

New MOM alerts still are forwarded to TEC and handled the same way. Microsoft has added some "guaranteed delivery" elements by way of acknowledgements between the two systems that the events were received. Any modifications of an alert generated by either system are reflected in the other system. Microsoft has even provisioned a mechanism to ensure synchronization by matching the MOM GUID for a particular alert with the Alert ID in TEC.

The MOM to Tivoli TEC Product Connector runs as a service on a system that has network access to at least one MOM 2005 management server in your MOM

configuration group. The Tivoli endpoint code must be installed on the server with the product connector service as it is used to communicate within the Tivoli Management Region (see Figure 11.6). The product connector uses a Web service for communication with MOM, and the Microsoft Connector Framework (MCF) must be installed on the MOM 2005 server.

Figure 11.6 Anatomy of a Tivoli Management Region



Connecting MOM to IBM Tivoli TEC

Connecting MOM to IBM Tivoli TEC is a matter of two steps: installing the software for the product connector and configuring both Tivoli TEC and the product connector to work together. You can install the connector on a MOM 2005 server or on a dedicated server as a stand-alone component. It is recommended, though, that you install the connector on a MOM 2005 management server with the MCF component installed to reduce system count and solution complexity without reducing the connector's ability to handle a high load of alert transfer between management platforms.

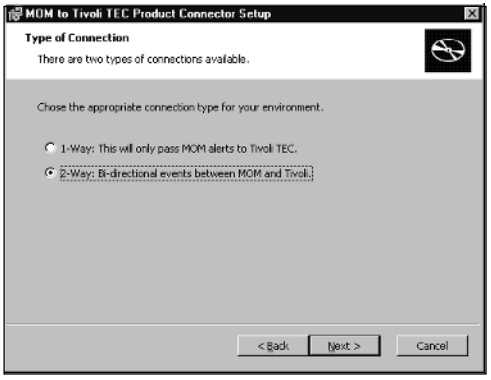
Installing the MOM to Tivoli TEC Product Connector

The installation of the MOM to Tivoli TEC Product Connector is straightforward. The following steps outline the install procedure:

1. Run **MTPC.msi** from the installation point.

2. The Welcome screen includes general information about the MOM to Tivoli TEC Product Connector. Click **Next** to continue.
3. The End-User License Agreement displays the license agreement for using the MOM to Tivoli TEC Product Connector. Click **I accept the terms in the License Agreement**, and then click **Next**.
4. On the Choose Setup Type screen, click the type of setup you require for the MOM to Tivoli TEC Product Connector.
5. On the Custom Setup screen, you can choose the MOM to Tivoli TEC Product Connector installation path. To choose the location, click **Browse**.
6. On the Change Current Destination Folder screen, enter the folder name of the location where setup should install the connector files.
7. On the Type of Connection screen, you can select what type of connection you will use when the MOM to Tivoli TEC Product Connector is set up. If you select 1-Way, then MOM will only forward alerts to TEC. If you select 2-Way, then MOM and TEC can communicate events between each other. If MOM updates an event, the event will also be updated in TEC, and vice versa (see Figure 11.7).

Figure 11.7 Selection for Type of Connection



8. On the Define MOM DCAMs screen, you can enter up to five MOM 2005 servers to be configured with the MOM to Tivoli TEC Product Connector. If you install the MOM to Tivoli TEC Product Connector on a MOM server, then DCAM1 is automatically filled in. The installation automatically imports the MOM to Tivoli Management Packs on your MOM 2005 server, and Setup skips to step 11 when you click **Next**.

9. The Additional Configuration screen describes the requirements to import the MOM to Tivoli TEC Management Packs into the MOM server database. This process must run when the installation completes. Click **Next**.
10. The MOM to Tivoli TEC Product Connector runs as a service and needs a user with rights to install, start services, and stop services. This user must be a member of the MOM Administrators group. This account must be a domain-level account or the service will not install.
11. On the MOM to Tivoli TEC Product Connector Service screen, you can have the MOM to Tivoli TEC Product Connector start the service after the installation completes. To start the service automatically, check **Start service after install**. To start the service manually, ensure that the check box is cleared. Click **Next**.
12. On the Ready to Install screen, ensure that all settings are correct, and then click **Install**.
13. When prompted, click **Finish** to complete the installation.

Configure Tivoli and the Product Connector

Once the MOM to Tivoli TEC Product Connector is installed, the Tivoli TEC configuration must be updated to support the product connector. This section assumes that you have already deployed the following requirements:

- Tivoli Framework 3.7.1 or 4.1
- Tivoli Enterprise Console Adapter Configuration Facility (ACF) 3.71, 3.8, or 3.9
- Tivoli Enterprise Console (TEC) 3.7.1, 3.8, or 3.9

There are several key configuration items that must be addressed before the connector will function correctly. From the Tivoli desktop, you must configure:

- MOM Roles
- The Microsoft Operations Manager policy region
- TEC for MOM. This is done using one of eleven MOM tasks that are accessible from the Tivoli desktop under the MOM policy region (ConfigureTECMOM).

Configuring the aforementioned items sets up the event server to interpret and process events from the MOM Administrator Console. The remaining tasks are to

provide a mechanism to deliver events from MOM to TEC and from TEC to MOM. This is done by distributing a TEC adapter created during the MOM to Tivoli TEC Product Connector installation. The steps that follow outline the process of facilitating the flow of events between the two EMS platforms.

To distribute the adapter configuration that allows events to flow into TEC from MOM, open the Profile Manager named **MOM_ACP** to reveal **MOM_Adapter**. This profile must be distributing to the Tivoli endpoint running on the server with the product connector installed. This is accomplished by creating a subscriber to the Profile Manager using these steps:

1. Select **Profile Manager** from the menu.
2. Select **Subscribers**. This action opens a new window.
3. Select the appropriate subscriber from the Available to become Subscribers list and move it over to the Current Subscribers pane.
4. Click **Set Subscriptions** and then click **Close**.

With this complete, you are now ready to distribute the MOM_Adapter by dragging the adapter and dropping it on the endpoint subscriber you just created. To complete the two-way flow of events, you must configure TEC to automatically forward TEC events to a MOM 2005 server. This is accomplished by using the MOM_TEC_Automation task. Be sure to reference the appropriate endpoint label when executing this task, as the endpoint label must be the same as the server's host name.

Depending on your implementation of Tivoli TEC, you may have other tasks that you will want to execute other than those mentioned in this section (see Table 11.2 for a complete list of available tasks). For additional information, consult the MOM to Tivoli TEC Product Connector Users Guide 1.1 available on Microsoft's site.

Table 11.2 MOM Tasks Controlling Flow of Events and Acknowledgments

Task Name	Task Description
MOM_ACK_EVENT	The MOM_ACK_EVENT task is used by the TEC rules engine to acknowledge events received from a MOM Server. It should never be run directly by the user.
MOM_CREATE_EVENT	The MOM_CREATE_EVENT task is used by the TEC rules engine to create TEC events on a MOM Server. It should never be run directly by the user.

Continued

Table 11.2 continued MOM Tasks Controlling Flow of Events and Acknowledgments

Task Name	Task Description
MOM_ACK_STATUS	The MOM_ACK_STATUS task will inform the user if the acknowledgment of MOM events is turned on or off.
MOM_TURN_ON_ACK	The MOM_TURN_ON_ACK task will turn on acknowledgements of MOM alerts being received by TEC. MOM acknowledgments are on by default.
MOM_TURN_OFF_ACK	The MOM_TURN_OFF_ACK task will turn off acknowledgments of MOM alerts being received by TEC.
MOM_TEC_EVENT_STATUS	The MOM_TEC_EVENT_STATUS task will inform the user if the flow of TEC events to the MOM Server is turned on or off.
MOM_TEC_EVENTS_ON	The MOM_TEC_EVENTS_ON task will turn on the flow of TEC events to the MOM Server.
MOM_TEC_EVENTS_OFF	The MOM_TEC_EVENTS_OFF task will turn off the flow of TEC events to the MOM Server.
ConfigureTECMOM	Used to configure TEC to receive MOM alerts.
MOM_TEC_Automation	Configures TEC to automatically forward TEC events to a MOM Server.
Manually_Forward_ TEC_Event	Manually forwards a TEC event to MOM.

Up to this point, we have discussed the configuration of TEC to allow the flow of events and alerts between the two management systems. Out-of-the-box, not much needs to be done in MOM 2005 itself since most of the business logic and configuration is done for you by the management pack. However, there are some settings that you may want to review to optimize or cater the functionality of the connector and the integration of TEC and MOM to best suit your needs and the needs of your organization.

Most of the configuration settings that are available are based on registry settings. Table 11.3 outlines the specific registry keys and values. Any change to these settings, though, will require you to stop and restart the MOM to Tivoli TEC Product Connector service.

Table 11.3 Configurable Registry Settings

Key (all under HKLM\Software\Microsoft\ProductConnector\)	Type	Description
Path	REG_SZ	Install path for MOM to Tivoli TEC Product Connector
ConnectorType	REG_DWORD	1=two way (default); 0= one way
MOMservers	REG_MULTI_SZ	List of MOM servers. Product Connector will attempt connection to each on startup and when a connection is lost. Format of entry is either computer name (such as MOMSERVER) or URL (such ad http://momserver/MCF/ConnectorService.asmx)
DebugLevel	REG_DWORD	Logging level. Default=5 All=1 Info=5 Warning=6 Error=7 Fatal=8 Off=9
DebugLogfile	REG_SZ	Debug log file. Default=Path + MOMprodConn.log
DebugMaxSize	REG_DWORD	Max size of log files in MB. Default=1
DebugLogFiles	REG_DWORD	Number of log files to keep (rollover). Default=3
AlertResultSet	REG_DWORD	Maximum number of alerts to receive at one time from MOM. Default = 100
AutoAcknowledge	REG_DWORD	Turn automatic MOM acknowledgement on or off. On=1, off=0 (default)
CacheExpiration	REG_DWORD	Number of elapsed seconds before cached alert entries expire if not acknowledged by Tivoli. Default=900
CacheLocation	REG_SZ	Location of cache file. Default=Path + MOMprodConn.cache

Continued

Table 11.3 continued Configurable Registry Settings

Key (all under HKLM\Software\Microsoft\ProductConnector\)	Type	Description
BookmarkSetting	REG_DWORD	Used when product connector starts, this is the number of hours to go back and look for alerts to be sent to Tivoli. Default = 0

Other Connectors from Third-Party Vendors

Several third-party vendors have developed their own solutions to fit an industry need, taking advantage of the integration possibilities that MOM 2005 offers. In this section, we will discuss connectors offered by eXc Software, a substantial partner with Microsoft for add-ons to MOM.

eXc Software has been building a library of Virtual Agents and Connectors to integrate common non-Microsoft technologies with MOM. Aside from their unique agentless approach to managing systems and devices, they also offer connectors for:

- HP OpenView
- IBM Tivoli TEC
- Micromuse Netcool
- CA Unicenter
- BMC Patrol
- BMC Remedy
- Nagios

As with the Virtual Agents that we discussed in Chapter 10, eXc Software's extension to MOM are based on their WMI non-Windows Event Provider, the base framework for all their solutions. The provider is installed on a MOM 2005 management server, as are the Virtual Agents and ConneXctors. No additional software is required to be installed on any other system or device.

In continuation, we will walk-through the general installation procedure for MOM 2005 running on a Windows Server 2003. This process is the same regardless of which ConneXctor you are installing. For the walk-through, we will install the

ConneXctors for CA Unicenter, importing the customized Management Packs, and configuring the ConneXctor to communicate with the CA Unicenter EMS.

Installation of the eXc Software Components

There are several requirements that must be satisfied before you can install any of the eXc Software components. Table 11.4 outlines the software requirements for an installation on Windows Server 2003.

Table 11.4 Software Requirements for Microsoft Windows Server 2003

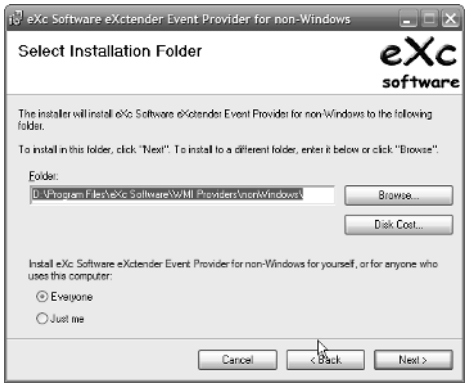
Windows Server Version	Requirement
Windows Server 2003	Microsoft Access 2000 or later * Network Monitor Tools * Simple Network Management Protocol * WMI SNMP Provider * WMI Windows Installer Provider Windows MSXML 4.0 or later Microsoft SOAP Toolkit 3.0

Note: "*" denotes that the component is installed through the Add/Remove Windows Components section of the Add/Remove Programs control panel applet.

Once the prerequisites are installed, you can perform the basic installation steps as follows:

1. Download the eXc Software Base Framework (or WMI non-Windows Event Provider) and the ConneXctor from www.excsoftware.com.
2. Install the eXc Software WMI non-Windows Event Provider using the *eXc_nonWindows_WMI_Provider.msi* Windows Installer package.
3. Select the installation folder. If you change the installation path from the default folder, you will have to make further modifications after the installation. You must select **Everyone**, or you will not be able to launch any of the Virtual Agents you install (see Figure 11.8).
4. Install the Red Hat Virtual Agent that you downloaded using the eXc_MOM_Caunicenter_Connector.msi Windows Installer package. Remember that if you changed the default install path for the event provider, you'll need to adjust the path for the Virtual Agent install folder as well. You must select **Everyone**, just as you did with the event provider install.

Figure 11.8 eXc Software WMI Non-Windows Event Provider Install Wizard



5. Since the ConneXctors rely heavily on SNMP to communicate with other EMS platforms, be sure to have both the **SNMP** and **SNMP Trap** services configured to start up automatically and running.

NOTE

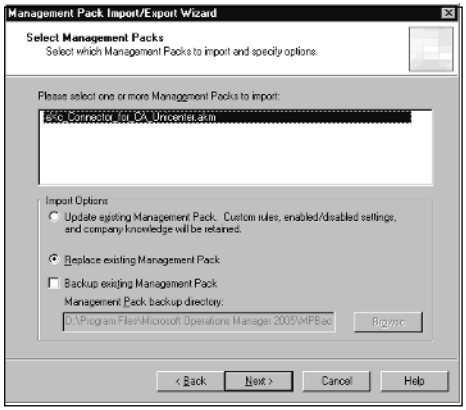
Before continuing with the rest of the process, the WMI non-Windows Event Provider must be fully configured. Refer to the configuration details outlined in Chapter 10 of this book for all the steps that must be performed.

Importing the Management Pack for the Connector

1. Import the Management Pack for the CA ConneXctor using the Import/Export Management Pack Wizard. This is launched by highlighting **Management Packs** on the left-hand pane of the MOM 2005 Administrator Console and right-clicking and selecting **Import/Export Management Pack**.
2. On the Select a Folder and Choose Import Type page, enter the path where you installed the ConneXctor for CA Unicenter.
3. Set the Type of Import to **Import Management Packs only**.
4. On the Select Management Packs page, select the **eXc_Connector_for_CA_Unicenter.akm** file.

5. Change the Import Options to **Replace existing Management Pack** and uncheck **Backup existing Management Pack** (see Figure 11.9).
6. When the import finished successfully, close the Import Stratus window.

Figure 11.9 Importing the Management Pack for the CA Unicenter Connector

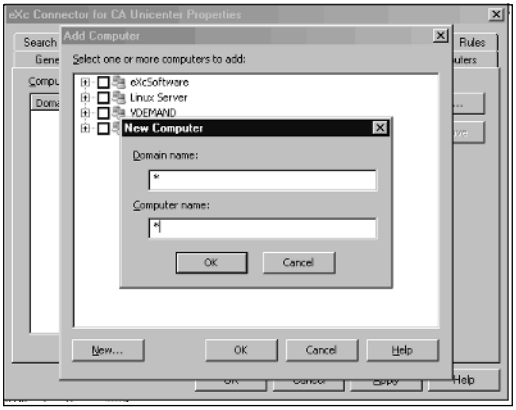


Configure the Management Pack for the Connector

The Management Pack for the CA Unicenter ConneXctor, by default, is not configured to forward any MOM alerts to Unicenter. You can select some (or all) of the MOM managed computers to be included in the Unicenter integration by including them in the eXc Connector for CA Unicenter computer group. To accomplish this, follow these steps:

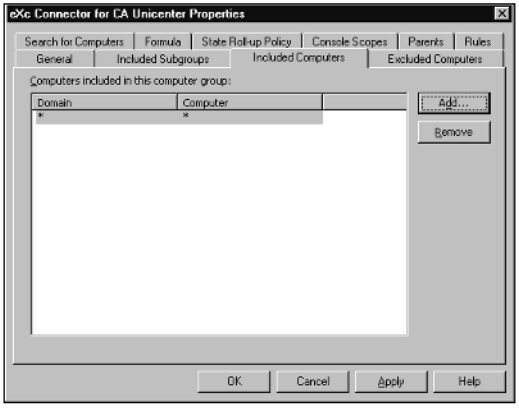
1. In the MOM 2005 Administrator Console, navigate the left-pane until you see the list of computer groups.
2. Highlight **eXc Connector for CA Unicenter**, then right-click and select **Properties**.
3. Select the **Included Computers** tab and click **Add**.
4. If you want to include only some of the computers, expand the appropriate domain(s) and select the computers to include.
5. If you want to include all the managed computers in your configuration group, click **New** to open the New Computer window. Enter "*****" for the Domain name and "*****" for the Computer name (see Figure 11.10).

Figure 11.10 Defining All Computers in the Connecter's Computer Group



6. Click **OK**, then **OK** again. Your Included Computers tab should look like Figure 11.11.
7. Click **OK** to close the computer group Properties window.

Figure 11.11 Including All Computers as Members of the Computer Group



8. Complete the configuration of the management pack by right-clicking on **Management Packs** and selecting **Commit Configuration Change**.

Some Independent Advice

For some organizations, key business decisions are made based on the status of your business applications and the systems they run on. In those circumstances, your EMS platforms, including MOM 2005, become critical systems for your company.

You can configure the connector to operate in a primary and backup role (by default, the product operates in stand-alone mode). This will give you a degree of high-availability if the primary and backup connectors are running on separate computers. To configure a fault-tolerant environment, you will need to install the connector onto two different computer MOM 2005 management servers. On both systems, you will need to use the eXc Software non-Windows Configuration Tool/GUI to set the Connector variables for the primary and backup roles. Define one computer as the primary computer by setting variable **g_strFailOverRole** to **PRIMARY** and the other computer as the backup computer by setting variable **g_strFailOverRole** to **BACKUP**.

Note that for this configuration to work properly, the primary connector will need to be able to send SNMP traps to the backup connector. Therefore, ensure that the associated SNMP read and write community variables are defined with proper values for your environment.

With the management pack configured, the Connector itself needs to be configured based on your requirements and environment. You must configure both the MOM side of the connector as well as the non-MOM side (the EMS). You can use the general guidelines that follow as a point of reference; however, your exact configuration will be based on how you want to use the Connector.

Configuring the MOM Side of the Connector

You must configure the Connector by specifying values for certain variables. This is done by using the eXc Software non-Windows Configuration Tool/GUI to set the connector global variables (see Figure 11.12). Table 11.5 lists the variables that can be configured.

Table 11.5 Configuration Variables for the eXc Software ConneXctor

Variable Name	Description
g_strXComputerName (where X is the name of the connector)	The DNS name of the computer running EMS (non-MOM management server)
g_strSNMPReadCommunity	The target EMS SNMP read community
g_strSNMPWriteCommunity	The target EMS SNMP write community
g_strMOMVersion	The MOM version, which can be either MOM2000 or MOM2005 (default)

Continued

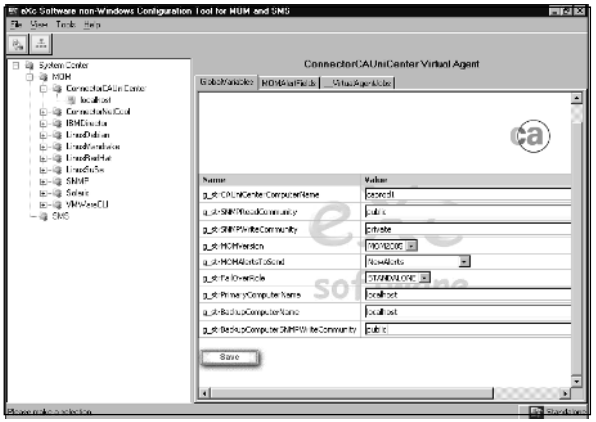
Table 11.5 continued Configuration Variables for the eXc Software ConneXctor

Variable Name	Description
g_strFailOverRole	The operating mode of the connector, which can be either STANDALONE, PRIMARY, or BACKUP

If **g_strFailOverRole** is either PRIMARY or BACKUP, then you must specify values for variables:

- g_strPrimaryComputerName
- g_strPrimaryComputerSNMPReadCommunity
- g_strBackupComputerName
- g_strBackupComputerSNMPWriteCommunity

Figure 11.12 Using the eXc Software Configuration Tool to Configure Connector's Global Variables

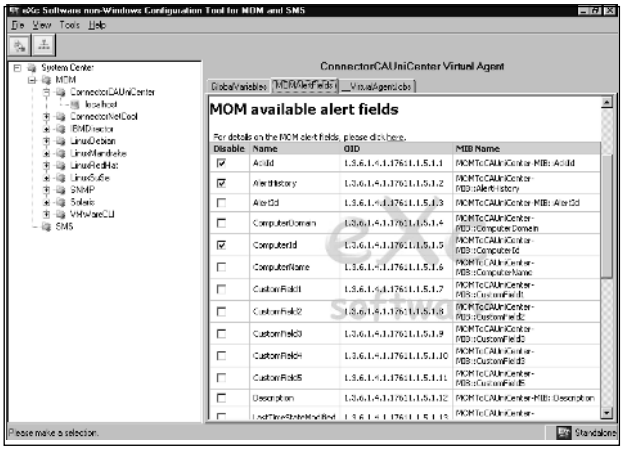


Configuring the Non-MOM Side of the Connector

Configuring the non-MOM side of the Connector, which we will call the target EMS, (i.e., Netcool, HP-OV, BMC PEM, CA Unicenter, etc.) involves configuring the product to receive SNMP TRAPs sent from MOM 2005 to the target EMS system. There is a mib file in the mibs subdirectory called MOMTo[ProductName]-MIB.txt. For example, the Netcool mib file is called MOMToNetCool-MIB.txt. The appropriate MIB needs to be compiled on the target EMS system. The target EMS

system needs to be configured to receive (accept) TRAPs that arrive with the eXc Software OID. Figure 11.13 shows the configuration of the alert fields and how they map to the SNMP OIDs of the Connector's MIB.

Figure 11.13 Alert Fields Available for the Connector MIB



If you want the connector to work bidirectionally, you must also enable the product to be able to send SNMP TRAPs to the MOM computer running the connector solution. Each target EMS has its own way of sending and receiving SNMP TRAPs so this section is very particular to the product you are connecting MOM 2005 to. As an example, in Netcool, you must modify the rules file (see file Recv_MOM_Traps.txt) and restart the trap daemon. For whichever product you are connecting MOM to, please consult the target EMS' documentation on how to receive and process SNMP TRAPs.

Once you can send SNMP traps from the target EMS, follow these steps for each alert that gets forwarded to MOM:

1. Populate OID 1.3.6.1.4.1.17611.1.3.1.3 with the MOM alert id.
2. Populate OID 1.3.6.1.4.1.17611.1.3.1.28 with the Action you want MOM to perform. This value can be INSERT, REMOVE, or CHANGE. If you have additional requirements, the Action scheme can easily be changed by modifying the function **SendTrapToMOM2** in the script *MOMReceiver.js*.
3. Optionally, if you want to store relational information to link the MOM alert ID, or GUID, and the target EMS alert ID, configure the target EMS to pass its alert ID to MOM in OID 1.3.6.1.4.1.17611.1.3.1.29. This will have to be configured outside of the eXc Software Configuration Tool/GUI because field 29 does not appear on the MOMAlertFields tab.

Running the Connector

By default, alerts are performed only when you change the resolution value for the specific alert. You may want to create a processing rule so alerts that meet a specific criteria, such as severity level, are forwarded to the target EMS automatically. This can be done by creating a new alert rule associated with the Connector's computer group, and configuring a custom response script to run when the criteria is met.

The following is an example of a script that automatically forwards all new MOM alerts that have a severity level higher than Error. This example is included with the installation of the Connector.

```
'AlertLevels:
'10 - Success
'20 - Information
'30 - Warning
'40 - Error
'50 - Critical Error
'60 - Security Breach
'70 - Service Unavailable

If (ScriptContext.IsAlert()) Then
   Set objAlert = ScriptContext.Alert
   If (objAlert.ResolutionState = 0) Then
      If (objAlert.AlertLevel > 40) Then
         If (objAlert.GetCustomField(5)<>"SentMOMAlert") Then
            objAlert.ResolutionState = 9

'If you would like repeated alerts forwarded as well,
'comment out the next line

            objAlert.SetCustomField 5,"SentMOMAlert"     'Mark as processed
         End If
      End If
   End If
End If
```

For greater information on customizing the ConneXctor for your targeted EMS, refer to the documentation from eXc Software available on its Web site.

Best Practices According to eXc Software

By default, the connector sends the entire MOM alert data defined to the other enterprise management system as a SNMP version 1 trap. If you want to change this, you will need to edit function **ProcessNewAlertsReceivedFromMOM** in file **MOMSender.js** located in the installation folder for the ConneXctor solution that you installed.

Similarly, if you want to customize the data from the other enterprise management system being received and sent to MOM, you will need to change the function **PopulateTheArray** in file **MOMReceiver.js**, also located in the same installation folder.

Summary

Whether you choose to use a Microsoft product connector or a commercial product from a third-party software vendor, integration from MOM has never been easier. This chapter focused on:

- The fundamentals of the connector technology, based on the web-service enabled Microsoft Connector Framework (MCF)
- Microsoft's solutions to connect MOM 2005 to HP OpenView and IBM Tivoli TEC
- Solutions available from eXc Software, the vendor with the largest library of add-ons for Virtual Agents and EMS Connectors

Large and small organizations have found real value in having single points of reference for the status of their critical infrastructure components. The inefficiencies of having multiple consoles and tools to view those resources have been eliminated by integration strategies and solutions. Thanks to technologies such as Web services, disparate products can now share information with one another, allowing a form of synchronization of different systems management platforms.

Microsoft and their partners have realized the demand for such efficiency gains, and they have developed powerful products that help organizations extend the benefits of MOM 2005 with such integration with EMS platforms such as HP OpenView, CA Unicenter, and Tivoli TEC.

Solutions Fast Track

Overview of the Microsoft Connector Framework

- ☑ As the foundation of the Microsoft product connectors and many of the third-party solutions, the MCF is the central most critical component for the integration with MOM 2005.
- ☑ The framework exposes flexible operations that are accessible through Web service calls using the SOAP protocol. Since SOAP support is standard in most development environments today, this creates countless opportunities to extract or insert information such as alerts and events from MOM.

MOM to HP OpenView Operations Product Connector

- ☑ Using standard Web service calls, Microsoft's MOM to HP OVO Product Connector offers a one-way solution to integrate MOM alerts into HP OpenView.
- ☑ Be sure to install the HP OpenView Interconnect (HP OVI) on at least one of the HP OVO servers, regardless of the operating system OpenView is running on.
- ☑ For smaller deployments, install the MOM to HP OVO Product Connector on the same MOM management server where the MCF is installed. This will lead to simpler installation and maintenance of the connector overall.

MOM to IBM Tivoli TEC Production Connector

- ☑ This is one of the most complicated connectors available, which accounts for its power and flexibility. Essential to the functionality of the MOM to Tivoli TEC Product Connector is the Tivoli configuration itself.
- ☑ As a two-way solution, be sure to take advantage of this product connector's deployment by allowing alerts generated in TEC to be forwarded to MOM as well. This allows MOM administrators to use the Operations Console as a single view into the enterprise.

- ☑ Out-of-the-box, this connector probably will not meet your needs. Be sure to reference the Tivoli TEC documentation as well as the documentation that is included with the MOM to Tivoli TEC Product Connector to determine which parameters must be tweaked to get the full value out of the product and meet your organization's needs.

Other Connectors from Third-Party Vendors

- ☑ Third-party solutions from vendors bridge the gap by delivering connector solutions otherwise unavailable that are generally simple to install and maintain.
- ☑ If you already have an investment in a third-party framework, such as the WMI non-Windows Event Provider by eXc Software, use the same framework to connect MOM 2005 to your enterprise management systems.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Does Microsoft make a MOM Connector add-on for all popular enterprise management systems?

A: No, currently Microsoft makes a product connector only for HP OpenView and IBM Tivoli TEC.

However, there are many partners such as eXc Software and Skywire Software, that have connectors and integration solutions available, covering a wide range of EMS platforms. Each vendor has designed their connector in a unique way, so you should evaluate more than one to identify the one that best meets your needs.

Q: Our EMS is managed by another team, who is not a fan of Microsoft technology. We are having a hard time getting them to assist with setting up our MOM connector. Is there anyway we can set up the connector without their help?

A: The answer is both yes and no. You can configure some of the commercially available connectors to send basic SNMP traps to your enterprise management system for all or only specific MOM alerts when raised, just as you would for a single server system. However, depending on how your EMS is configured, it may discard traps received from unknown origins (this is the behavior of HP OpenView, for example). Also, if they do not compile a specific SNMP MIB, the alerts they receive will be in raw OID format, which aren't very useful in most situations.

Q: We use HP OpenView in our organization. Is there a licensing cost associated with deploying the MOM to HP OVO Product Connector?

A: No. Microsoft offers the MOM to HP OVO Product Connector as a free add-on to MOM 2005. In fact, the component required on the OpenView side, HP OVI, is also a free tool available from HP. As long as your OpenView installation is licensed appropriately, there are no additional costs.

Q: Some of the product connectors seem extremely complicated to set up and maintain. Isn't there an easier way to get my MOM alerts into my EMS to make it a single view of our enterprise?

A: Yes. Not all the solutions require multiple components to be installed on both sides of the connector. eXc Software's solutions are rather simple, and they follow the sample general installation and configuration steps regardless of which connector you need for your EMS. Using SNMP objects built into Windows and precompiled mibs for your EMS, most eXc Software connector solutions can be deployed quickly and with little hassle. That doesn't mean that it's not powerful, though. You can customize the connector as your requirements change and your needs grow, creating a very intricate solution.

Q: I think MOM 2005 is one of the most powerful and flexible management systems out there. Can't I use MOM as my central EMS rather than extracting its alerts and forwarding it to another EMS?

A: Yes, you can. The basic function of any connector is to send information from MOM to another EMS. However, you can pull information from other EMS platforms into MOM provided that the connectors that you will be using support two-way communication with MOM. Many products, including the MOM to Tivoli TEC Product Connector, allow both MOM and the targeted EMS to stay in sync with one another, meaning that you could use either the EMS console or the MOM Operations Console to view the status across your enterprise. Regardless of which system originated the alert, both platforms should show the current status, including acknowledgments.

Chapter 12

Planning for Microsoft System Center

Solutions in this chapter:

- **What Is Microsoft System Center?**
- **About System Center Components**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

At this point in the book, you should have a good understanding of the features and functions of Microsoft Operations Manager 2005. You can now see that MOM is a very robust, powerful tool that can make your life and the lives of your IT staff much easier. Now, what if we told you that MOM was only a piece of a much larger puzzle, intended to further help you with the management and stabilization of your IT enterprise systems? In this chapter, we will introduce you to the concept of Microsoft System Center, and give you a little background on what makes up this offering.

What Is Microsoft System Center?

Microsoft System Center is an initiative by Microsoft, built around the framework of the Windows 2003 operating system and a variety of Microsoft Systems Management products. Each of the products that are part of System Center has been developed to complement the others, allowing for easy integration and seamless administration. System Center is intended to assist IT professionals in several key areas:

- Capacity planning
- Change management
- Data protection
- Operations management
- Problem solving

Many of the products intended to be part of System Center have already been developed and released, whereas others are still in beta testing (as of the writing of this book), and more are on the horizon with expected release dates in the foreseeable future. The products currently in release and in development (at least, those publicly announced) are:

- Microsoft Operations Manager 2005
- System Center Data Protection Manager
- System Center Reporting Manager 2006 (currently in Beta)
- Systems Management Server 2003

As part of the System Center initiative, Microsoft also offers a tool for planning your deployments of certain Microsoft products, known as System Center Capacity Planner 2006. This tool is very handy for not only deploying parts of the SC family,

but other Microsoft products such as Exchange 2003. Capacity Planner can help in a variety of areas including performance planning, infrastructure planning, reporting, and cost analysis.

As mentioned earlier, System Center is an initiative that is currently underway, and is expected to continue for the foreseeable future. Because of the complexity and size of the initiative, Microsoft has decided to release System Center in a series of "waves."

Some Independent Advice

Microsoft continues to move the scope and components of System Center. If System Center is an initiative that you would like to bring into your organization, we highly recommend visiting Microsoft's System Center Web page www.microsoft.com/windowsserversystem/system-center/evaluation/overview/default.mspx on a frequent basis. Also, if you plan to download any of the betas, keep in mind that Microsoft is notorious for removing functionality from betas and release candidates before they go to full release.

Defining the System Center Waves

Obviously, the amount of time and resources that goes into enterprise-wide products limits the ability for a manufacturer to release a multiheaded solution such as System Center. In an effort not to rush products to market in order to provide stable, secure releases, Microsoft has made the decision to roll out System Center in three separate waves. Each wave represents a milestone in the product lifecycle of System Center. Microsoft outlines the waves as follows:

- **Wave 1** Consists of the already-released Microsoft Operations Manager 2005, Systems Management Server 2003, and the soon-to-be-released Systems Center Reporting Manager 2006. We will discuss each of these in some depth later in this chapter.
- **Wave 2** In some respects, Wave 2 is already underway. Wave 2 is intended to support the rollout of capacity management tools (as we discussed earlier), integrated management tools for midsized companies, and the next releases of MOM and SMS. Microsoft targets the completion of Wave 2 in the 2006-2008 time frame.

- **Wave 3** Wave 3 is still a little fuzzy at this time; however, Microsoft expects that Wave 3 will focus around model-based management of distributed services and applications.

Now, let's take a look at some of the components that are available for use today and in the immediate future.

About System Center Components

Obviously, to get into a full description of the other components of System Center would require another book (or two) to cover all the details. We can, however, still touch on some of the high points around the other components (besides MOM 2005) that make up System Center. In this section we will cover three of the four components that we discussed earlier:

- Systems Management Server 2003
- Systems Center Data Protection Manager 2006
- System Center Capacity Planner 2006

Some Independent Advice

System Center Capacity Planner 2006, like System Center Reporting Manager 2006, is still in beta mode as of the writing of this book. Since they are still a beta version, you can expect some features to be added and removed before the final release is available. Keep checking the Microsoft System Center Web site for the status of these products.

We will begin this section with the System Center solution with the longest track record, SMS 2003.

About SMS 2003

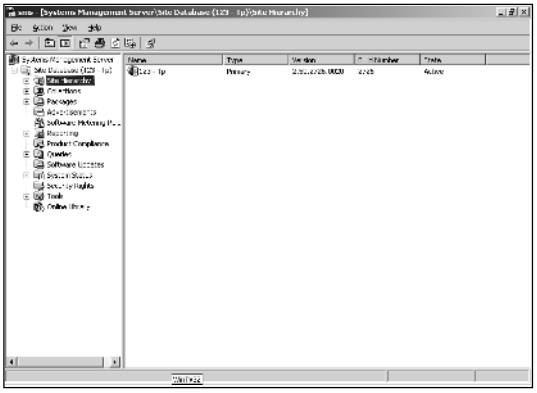
As you probably know, Systems Management Server has been around for a number of years and has gone through a number of changes over the years. As it has changed, it has gone from a package known for being more of a disaster than a solution, to a very reliable, stable solution for managing a wide variety of system functions within your environment. Instead of spending too much time talking about the previous versions of SMS, let's move right into an overview of the latest version of the Systems Management Server product, SMS 2003.

Overview of SMS 2003

SMS 2003 (see Figure 12.1) is focused on three key areas: change management, asset management, and configuration management. SMS 2003 can be used for a variety of functions:

- **Asset management** SMS can provide management in two key areas. First, since SMS has to install an agent on each machine that it manages, it has the ability to report back to the SMS server the specifics of the managed systems. SMS can provide detailed information on the client hardware platform, down to the BIOS revision! Second, SMS can help you stay in compliance with your software by reporting back on installed software to help you get a grasp on the types (and amount) of software installed on client systems.
- **Software deployment** Yes, Windows Group Policy Objects (GPOs) can be used to distribute software to clients, but SMS 2003 takes it a step beyond. SMS allows you to not only roll out the software, but also provides for the planning of the deployment via the SMS deployment planning tool. The planning tool assists with the planning of deployment by providing key reports on the environment, based on the aforementioned asset management.
- **Security patch management** Again, you're probably thinking, "Why do I need SMS for patch management when Windows Server Update Service (WSUS) is free?" Well, once again SMS goes a step beyond. Whereas WSUS ends at Microsoft products, SMS can be used to patch *any application that runs on a Windows platform*. This provides for a single solution for managing and updating all of your applications.

Figure 12.1 Systems Management Server 2003



At the risk of sounding like a used car salesman, that's not all! SMS has a number of additional features that we will cover in the next section.

What's New in SMS 2003

Many of you may be familiar with the previous incarnations of the SMS product. Some of you may have good memories, and some of you may have very bad memories. For many years, SMS was the "red-headed stepchild" of Microsoft. To Microsoft's credit, many of the issues you are familiar with from previous versions have been corrected. On top of the items that were corrected, there are a number of new items:

- Active Directory discovery
- Bandwidth-aware clients
- Application deployment planning
- Identification of system vulnerabilities
- Software inventory file level searching
- Support for Windows' Add or Remove Programs
- Vulnerability assessment and mitigation reporting
- Windows XP Remote Assistance support
- Wizard for patch deployment

Each of these features (as well as some not mentioned earlier in this chapter) has improved SMS tenfold.

Some Independent Advice

There are a number of great books available for SMS 2003. We recommend that if you are interested in learning more about the SMS 2003 product that you visit your favorite bookstore (or online bookstore) for more information. Alternatively, Microsoft's Web site offers an endless supply of useful information about SMS 2003. You can visit this site at www.microsoft.com/smserver/default.mspx.

SMS Feature Packs

Whereas MOM 2005 has its feature add-ins known as Management Packs, SMS 2003 has a similar offering known as Feature Packs. As the title would indicate, feature packs are intended to expand on the features and functions of SMS 2003. They are not service packs, but rather additional bells and whistles that can be added to the product post-implementation. Table 12.1 outlines some of these feature packs.

Table 12.1 Systems Management Server 2003 Feature Packs

Management Pack Name	Management Pack Description
Administration Feature Pack	Contains tools for deploying applications with elevated privileges, copying setting between SMS sites, and managing accounts and passwords by SMS sites.
Device Management Feature Pack	Allows SMS 2003 to manage mobile devices running Windows CE.
Operating System Deployment Feature Pack	Allows for ease of deployment of Microsoft Operating Systems in an enterprise.

You can get more information about the management packs listed in Table 12.1 (as well as download them if you are interested in running SMS or learning more about it) at www.microsoft.com/smserver/evaluation/featurepack/default.mspx. You can also pick up a 120-day evaluation copy of SMS 2003 at www.microsoft.com/smserver/evaluation/2003/default.mspx.

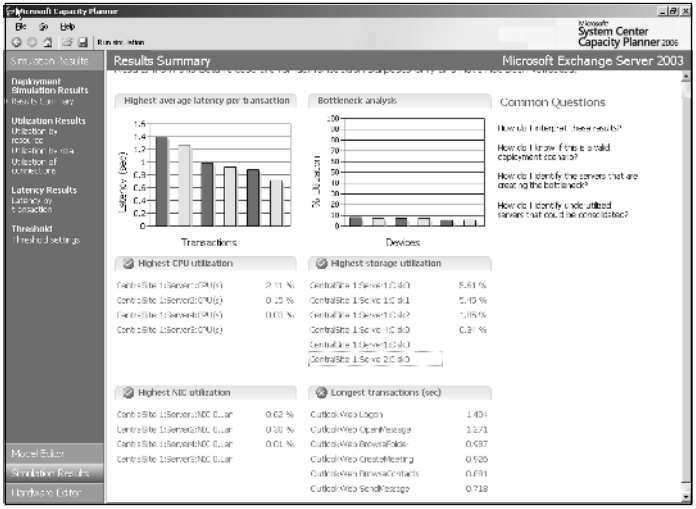
About System Center Capacity Planner 2006

System Center Capacity Planner 2006 (see Figure 12.2) is intended to be the replacement for those know-it-all consultants who are contracted to tell you exactly how to plan a rollout in your environment. OK, so that might be taking it a bit far, but it does assist you in working out various hardware and software scenarios relating to Exchange 2003 and Microsoft Operations Manager 2005 rollouts.

Figure 12.2 Systems Center Capacity Planner 2006

By using the Capacity Planner wizard, you can outline your environment by punching in some key information about your current environment, hardware preferences, and other tidbits of information. The Capacity Planner will process the information that you have provided, and return a potential rollout scenario (see Figure 12.3).

Figure 12.3 Systems Center Capacity Planner Results Page



A typical system architecture model consists of the following information:

- Hardware: server specifications (single processor vs. dual processor, memory, SAN attachment, etc.)

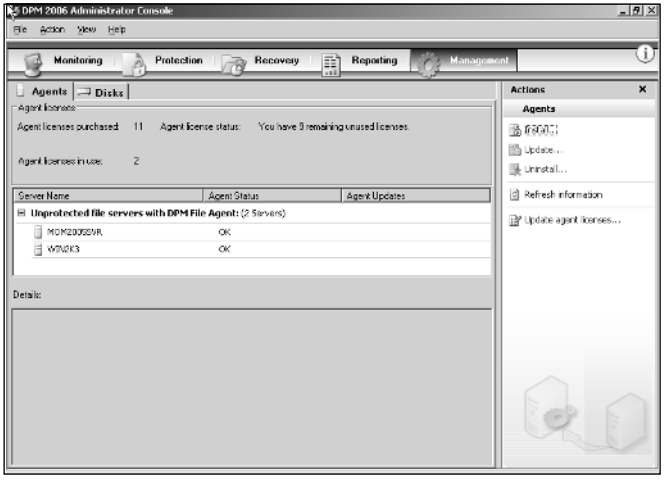
- Software server types (SQL, Exchange, Domain Controllers, etc.)
- Topology: WAN speeds
- Usage profile: site usage and client usage

After your initial pass-through with anticipated configurations, you can save your results and continue revisiting and tweaking them as you work through your potential rollout. As of the writing of this book, this tool is still in Beta Refresh; however, you can pick up a copy at http://www.microsoft.com/windowsserversystem/systemcenter/evaluation/capacity/default.mspx.

About System Center Data Protection Manager 2006

Data Protection Manager 2006 (see Figure 12.4) is a new offering from Microsoft intended to provide data protection and recovery by using disk-based solutions, such as replication and Microsoft's Volume Shadow Copy. Data Protection Manager currently works with Windows 2000 Server, Microsoft Windows Server 2003, and Windows Storage Server 2003. DPM is a policy-driven engine used to provide IT enterprises with better control of their recovery infrastructure, continuous protection, and rapid data recovery, without the need for expensive data recovery methods.

Figure 12.4 Systems Center Data Protection Manager 2006



According to Microsoft's Data Protection Manager Web site, the ideal DPM customers are *"medium-sized data centers that have between 5 and 49 servers and that have the following characteristics*":

- Significant backup window issues—for example, a costly and inefficient backup solution with "no good time for a backup."
- Frequent file recoveries from tape. For example, five to ten recoveries per month.
- Familiarity and/or experience with the benefits of Volume Shadow Copy Service (VSS) or the Shadow Copies of Shared Folders features of Windows Server 2003.
- A Recovery Point Objective (RPO) of approximately one hour or less. A RPO is the amount of data a customer can afford to lose without affecting business viability.
- A faster Recovery Time Objective (RTO) than tape can provide. RTO is the time required to recover files.

Some Independent Advice

Microsoft has a great in-depth introductory white paper entitled *Introduction to Microsoft® System Center Data Protection Manager 2006*. The direct link to the document is http://download.microsoft.com/download/c/4/c/c4c22a50-247e-4249-a9f7-a6481d4fa947/DPM_Introduction.doc; however, you can find the document on the DPM Web site at www.microsoft.com/windowsserversystem/dpm/default.mspx.

Summary

This chapter was intended to give you a taste of some of the tools currently available and coming soon from Microsoft that are intended to work hand-in-hand with Microsoft Operations Manager 2005. Many of these tools can greatly improve your ability to manage and defend your enterprise from a variety of issues, starting at the design phase, all the way through implementation. A few things to remember with the System Center tools:

- Not all tools are currently available, and features in the beta versions may not carry over to the full release.

- SMS 2003 is the most senior of the System Center tools, and therefore is the most robust with the possible exception of MOM 2005.
- Each tool should be used as only one piece of a much larger systems and network architecture design.

Microsoft System Center is your Swiss Army knife for managing your Windows-based enterprise environment. Each tool assists you with the ability to reduce your administrative burden while increasing your ability to understand exactly how the machine is running. System Center is being deployed by Microsoft in a wave approach, meaning that different applications (and revisions) will be released over a number of years. However, beta versions are currently available and can be downloaded and reviewed to determine if they may be a good fit for your organization once released.

Solutions Fast Track

What Is Microsoft System Center?

- ☑ System Center is intended to assist IT professionals in several key areas: capacity planning, change management, data protection, operations management, and problem solving.
- ☑ The products currently in release are Microsoft Operations Manager 2005, Systems Management Server 2003, and Data Protection Manager.
- ☑ The products currently in beta testing are System Center Reporting Manager 2006 and System Center Capacity Planner.
- ☑ System Center will be deployed in three separate waves.

About System Center Components

- ☑ Three key areas of Systems Management Server 2003 are asset management, software deployment, and security patch management.
- ☑ Microsoft System Center Capacity Planner 2006 helps size and plan deployments of Microsoft Exchange Server 2003 and Microsoft Operations Manager 2005.
- ☑ Data Protection Manager 2006 is intended to provide data protection and recovery by using disk-based solutions, such as replication and Microsoft's Volume Shadow Copy.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Will System Center be packaged and sold by Microsoft resellers?

A: No, or at least this is not planned at this time. Since System Center will be deployed in waves, each component will be available separately.

Q: When will the beta versions be available in final release?

A: This varies by software. Your best bet is to keep checking back on the System Center Web site for updates and news.

Q: Where can I get a copy of System Center Reporting Manager 2006 beta?

A: You can request to become a beta tester at http://beta.microsoft.com.

Q: Does MOM have management packs for SMS?

A: Yes, there are a number of free SMS Management packs for MOM available on the MOM Web site.

Q: Data Protection Manager sounds like a great tool. What is the price?

A: Great news, it's free!

Chapter 13

Troubleshooting MOM

Solutions in this chapter:

- Using the MOM Resource Kit
- Troubleshooting Management Packs
- Backing Up and Restoring a MOM Server

- ☑ Summary
- ☑ Solutions Fast Track
- ☑ Frequently Asked Questions

Introduction

At this point the entire MOM infrastructure should be doing exactly what you had planned before the implementation. But things that can go wrong sometimes do; this is also the case with a complex product like MOM. And when MOM runs badly, there is often a lot of digging required to find the solution. To help you with the digging, there are a lot of tools that will give you the information you're searching for. The goal of this chapter is to give you a good grasp of turning the "bad" MOM into the "nice" MOM.

Using the MOM Resource Kit

To be able to troubleshoot the MOM environment there are a lot of places to start looking. But there is one tool you can't afford to miss: the MOM resource kit tools. These tools are all used to troubleshoot the MOM infrastructure. Some of the tools in this Resource Kit make it possible to extend the current functionality in MOM even further. This makes it not only a great tool to troubleshoot, but also a necessary component of a complete working environment. You can find the MOM Resource Kit at www.microsoft.com/mom/downloads/2005/reskit/default.mspx.

The MOM Resource Kit is separated into five sections, each containing specific tools or documents. However, when you download the Resource Kit, only three of the five will be in the installer pack. The following sections list the various tools in the Resource Kit.

Management Pack Toolkit

This toolkit is used for creating, editing, and troubleshooting management packs. It includes the following tools:

- Business Activity Monitoring (BAM) Wizard
- Configure Action Account
- Convert Management Packs to XML (MP2XML)
- Event Creator
- Managed Code Response Utility
- Management Pack Differencing Tools
- Management Pack Version Checker
- Management Pack Wizard

- Remove Blank Names
- Resultant Set of Rules
- Rule and Computer Group Toggle Utility

Troubleshooting Tools

This part is used to troubleshoot your MOM infrastructure. It includes the following tools:

- Clean up MOM
- Management Group Utility
- MOM Information Utility
- MOM Inventory
- MOM Trace Log Viewer
- Windows Server Cluster Detection Utility

Power Tools

This part is used to troubleshoot your MOM infrastructure. It includes the following tools:

- Agent Helper
- Operator console Notifier
- Password Updater
- SharePoint Web Part
- Task Launcher

SOME INDEPENDENT ADVICE

If you're starting to work with a fairly large MOM environment, you should have a test system set up. This does not have to be a big server, but it should be sufficient to meet your testing requirements. To get the input data for the test environment, you can use the multihomed feature of the agents. This makes it possible to separate the rule sets for the test and production environment.

Shortcuts…

Operator Console Notifier

In the Power Tools there is a tool called Operator Console Notifier. This is a great tool if you do not want to stare at the MOM console all day. When this tool is installed, the Operator Console Notifier is added to the start menu folder, and an icon is placed into the tray area of the task bar.

This tool performs like the Outlook 2003 e-mail notifications. If the status of one of the monitored servers has changed, the Operator Console Notifier will pop up (see Figure 13.1).

The information provided by this tool is amazing. First, we can see the bold status is the one that has changed. The arrow on the right of this status gives a clue about the number of server that has its status raised or lowered. However, it is not possible to know how many have changed. If you find you need to take a look at the Operator console, only one click on this screen is enough to open it. And even the configuration is simplistic: None.

This is by far the most valuable tool in the resource kit. If I implement MOM at a customer site I always tell them about this tool and it always gets implemented.

Figure 13.1 The Operator Console Notifier in a Pop-up State

Overview of MOM Troubleshooting Tools

There are troubles in the MOM infrastructure, and yes, you're the one who is going to solve them—or even better, solve them *fast*. Because MOM is a system that monitors your corporate network and server, there are very legitimate reasons to make sure it runs smoothly and in optimal form. The moment your system is not running

smoothly and in optimal form great stakes are involved. Just imagine explaining your CIO about missing the crash of the seconded disk in the Raid array of your online Web database, "because MOM was not running the way it is supposed to run." The first question you will get is: "How is it possible that the Monitoring system is not monitoring after investing all this money?" This is not the place you like to be. So we better make sure the MOM infrastructure is running smoothly and in optimal form again as fast as possible

Cleanup MOM

Cleanup is one of those tools that you wish you didn't need to use. This is the stick of dynamite in your MOM infrastructure. It can do great work very fast, but be (very) careful where to use it. In real life I have run into issues during the deployment of the agents on the server, due to the pilot installation of MOM in the network. Somehow the agent used in the pilot environment was not removed completely, causing the new agent installation to fail. After running the CleanupMOM.exe /z:"A" the server was cleaned of any information about the agent installed, and the new installation ran fine.

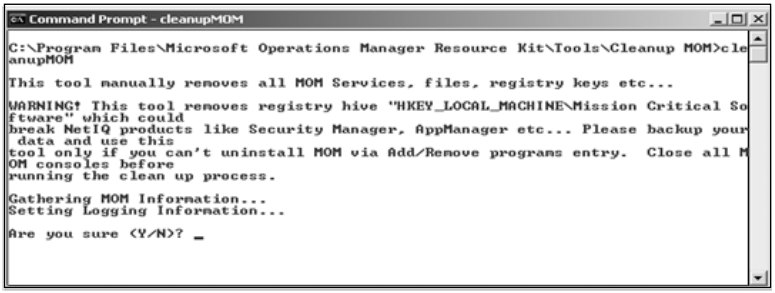
The Cleanup MOM tool is used to do a brute force removal of the MOM entries and programs on the server. It does not look at the role of the server in your MOM infrastructure. If you run this tool on your Monitoring Server it *will* remove MOM in the most uncomfortable way. But the same goes for that nasty server on which you were unable to install the agent. Run this tool on this server and all references to MOM are removed from the registry, and 99 out of 100 times the agent will install.

The default of the CleanupMOM.exe is to remove all information on the server. But when you use the */z:*, you're able to target specific areas to remove:

- **All:** Removes all information about the presence of MOM on the server
- **S:** Removes all information about the presence of MOM Server components on the server
- **A:** Removes all information about the presence of MOM Agents components on the server
- **R:** Removes all information about the presence of MOM Reporting components on the server

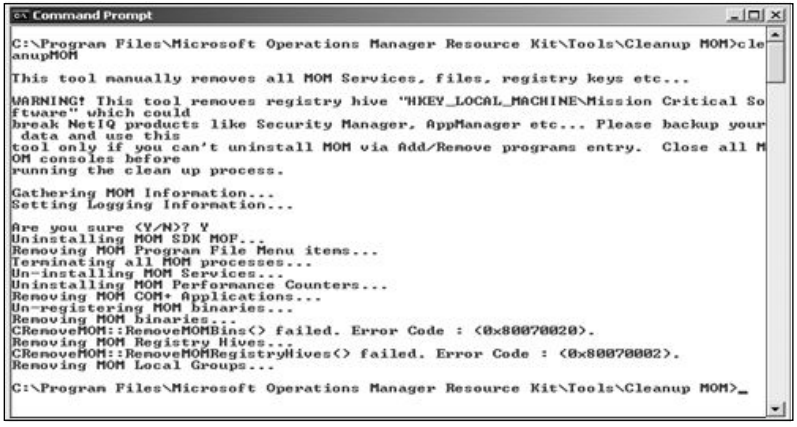
Running Cleanup MOM will give the information shown in Figure 13.2 on the screen. This information will give you a firm warning not to use this tool unless you're absolutely sure of what you're doing.

Figure 13.2 Running the CleanupMOM.exe Tool



After giving the final **Y** in answer to the question if we are sure the default behavior of CleanupMOM.exe will show (see Figure 13.3), all relevant information is destroyed. When I ran this tool, the MOM server in my test lab was running fine. This is an enormously powerful tool—use with care!

Figure 13.3 Running the CleanupMOM.exe Tool



If you have one or more agents that do not (re)install, this can be the tool to make them install correctly. First you need to make sure all references to the MOM agent are removed using the command **CleanupMOM.exe /z:A:**

Then try to rerun the agent installer. In most cases the installer will install successfully.

Management Group Utility

If you end up having a multihomed agent that is acting weird, the problem might lie in the configuration of the management groups that are corrupted. In such cases you need to be able to recover the agent. This can be done with the management Group

Utility (MGUtil.exe). Basically, you start by running the MGUtil.exe without parameters; this will give the management groups the agent reports to as a result.

It you suspect the agents have corrupted management group configurations, you can run the same tool using the MGUtil.exe with the **/c** parameter. This will result in a list of all the management groups configured (maximum of four) that are corrupted. If there is any management group or groups listed in response to this program, you can remove the configuration using the MGUtil.exe together with the **/r** parameter. After running this command the corrupted management group configurations are removed from the agent. The next step is to reinstall the agent.

MOM Information Utility

Using the MOM Information Utility is like having an all access pass to the MOM infrastructure. There are many things that can go wrong during the process between the event or performance counter happening and logging in to the database. During these times it is hard to see what is going on. This is where the MOM Information Utility comes in.

The MOM Information Utility can provide you with key information on all rules, responses, and VarSet information. In this case it will be retrieved from the agent. For example, you can compare the information from the server with it. Maybe that is a corrupt package in the queue—No problem, the MOM Information Utility is able to flush the queue for you (we're starting to sound like an infomercial, but there is more…). The MOM Information Utility is also able to put your MOM agent into maintenance mode and enable script debugging.

To use the tool there are a number of switches that need to be set to free the information:

- **MOMInfo.exe /rules /out:rules.xml** Results in the dump of all rules of all configured management groups in the rules.xml file. You can be more specific if you add the /config:managementgroup to receive the information about one management group.
- **MOMInfo.exe /responses /out:responses.xml** Dumps all running response to a file called responses.xml. You can be more specific if you add the /config:managementgroup to receive the information about one management group.
- **MOMInfo.exe /clearqueue** Results in the queues being emptied and the agent restarted. You can be more specific if you add the /config:managementgroup to flush only the queues of the management group mentioned.

- **MOMInfo.exe /maintenancemode** Puts the server into maintenance mode. Therefore, the server needs to communicate to the MOM server to give the status to the MOM console. However the server is put into maintenance mode.
- **MOMInfo.exe /scriptdebugging** Enables script debugging on the agent. This is the option you can use when you have trouble with a script that is not willing to execute on the agent.
- **MOMInfo.exe /errorhandling** Turns on error handling to get information when MOM crashes.

MOM Inventory

In case you have a real jam on MOM, there may be some support from Microsoft Product Support Services.

If you ever came across this situation, you know the drill. It all starts with gathering log files and other information that you probably never thought would be useful. This tool will do the digging for you. It will gather all kinds of logs and information and package it into one single cab file to send to PSS. This will save you the burden of browsing through the endless list of information to gather.

It will collect the following information for you:

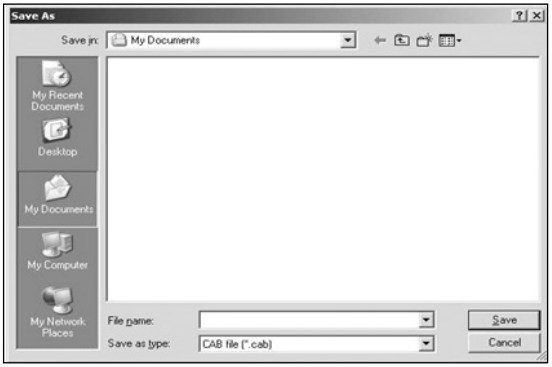
- All the Windows Installer logs for MOM
- MOM Trace Logs
- MOM Registry Information
- MOM Server Configuration (both local configuration and configuration stored in the DB)
- All running processes
- All NT Event Logs

Running the tool is as easy as one, two, three. Running MOMInventory.exe will display the screen shown in Figure 13.4.

Figure 13.4 MOM Inventory Start Screen

To start collecting, press **Run Collection**. You will be presented with a save file dialog that gives the location where the CAB file should be placed (see Figure 13.5).

Figure 13.5 Save CAB File



After you select the location and filename, the information is stored. During the collection the progress is displayed in a dialog (see Figure 13.6). After the collection is complete, click **Close**, and you're ready to send the information to PSS.

Figure 13.6 MOM Inventory Progress Dialog

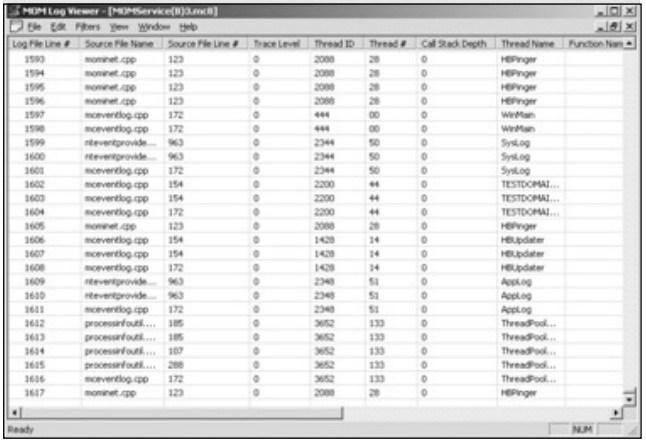
MOM Trace Log Viewer

Use the trace log viewer if you need to zoom in on the running history and trace logs on the MOM servers (see Figure 13.7). These log files, ending with the MC8 extension, can default and are found at the following location: %temp%\ Microsoft Operations Manager. If you run into trouble (e.g., with the rule processing of an agent), you're able to zoom in on all actions of the agent and server, thereby checking step by step where the process is failing.

Figure 13.7 Trace Log Viewer without Selected Log

Press **File -> Open** and browse to the selected log file. This will open the log file (see Figure 13.8).

Figure 13.8 Trace Log Viewer with Selected Log



Windows Server Cluster Detection Utility

Because clusters are not seen that often, you won't use this tool often. MOMClusterTool.exe is used to test how the MOM server detects the Cluster Resources that are configured as Virtual Server on a Windows Server Cluster. Therefore, you're able to check if the MOM infrastructure will work correctly with the cluster environment.

MOMClusterTool.exe will help diagnose why a Windows Server Cluster Virtual Server cannot be detected by MOM, by checking the specific configuration that MOM expects. This utility can be run on one of the servers in Cluster Group or run remotely against the cluster.

Troubleshooting Management Packs

Importing the management packs is only half the work that has to be done. After importing the management packs, you'll need to work on the alert tuning and the troubleshooting on the new management packs.

Troubleshooting management packs is not an easy task; an error can come from a lot of places in the MOM infrastructure. Earlier we talked about a lot of tools that can assist you in troubleshooting the management pack, as you will read in the following sections.

Best Practices According to Microsoft

- MOM management packs are created by the same people who wrote the code of the program it monitors. Therefore, you can safely assume that these people know what they are doing. Microsoft advises not to tweak the rules in the management packs unless you're absolutely sure of what you are doing.
- Because of the dependencies management packs can have, Microsoft recommends that you import only one management pack at a time.
- Be sure to check the management pack guides for every management pack you enroll in the MOM infrastructure. The dependencies are mentioned in the management pack guides. You can easily make a management pack deployment plan by drawing a treelike figure that displays the dependencies of the management packs.

Some Independent Advice

A lot of errors can be caused by timeout issues. The errors, "A script hung or exceeded its specified timeout," mainly are produced by servers that have a large load. This can easily be solved by changing the script timeout settings in the rule that caused the problem.

However, be sure to take note of this so you can change it back if the script does not time out but really hangs.

Shortcuts…

Lots of Errors after Importing a Management Pack

With a number of management packs there is a settle time needed to run properly. This is due to the discovery scripts (e.g., check the Active Directory layout). After importing the script you may notice a lot of errors coming from these packs. Ignore these for a day just to filter the settling errors. After the first day, start checking for real errors.

Troubleshooting Exchange Management Packs

This is one of the management packs I always have a hard time starting. When it works, it works like a charm and gives a rich set of information about the Exchange environment and performance. But getting it to work can be a real problem. If you get into the newsgroups and query about the errors in the exchange management pack, you will receive enough references from people with problems, too. Luckily very great care is taken in supporting the Exchange management pack. If an error occurs, there is always a clear description about the error and what the source could be. Besides that, every alert has a link in the knowledge base that points to the up-to-date information on the Microsoft Web site

Having said this, let's have a look into troubleshooting the Exchange management pack. Because of the high number of errors that can be caused by this management pack, I will address only a few. To completely describe all errors that can occur would take an entire book. If these are not the problems you are having, you need to resort to the Microsoft newsgroups for more information or make a support call. A separate Exchange management pack group exists.

ExMOM 8203 Alert

During the deployment it is possible that the ExMOM 8203 Alert will be logged in the MOM operator console. If this is the case you have stored a MOM monitoring mailbox on a front-end server. There is a simple solution to this one: move the mailbox to a backend server.

Permissions and Directory Access Errors

One of the things that often go wrong is access to the test mailboxes. If there is an access error, the mailbox availability monitoring will not work (as well as a lot of other things). This is one of the vital configurations that need to work.

One of the things that will show up in the Operator Console is an error in the MAPI logon verification script (9981 and 9016). With these errors you need to check if the mailbox access account has sufficient (full) access to the MOM test-mailbox. This can easily be done by connecting to the mailbox using the mailbox access account from Outlook.

This is only one of the many situations. The main point is that it is easy to test the access using Outlook.

Exchange Topology Discovery

It is possible to let the exchange management pack draw your Exchange infrastructure. This is fully automated, but needs some configuration to work.

You need to add an Exchange server manually to the Microsoft Exchange Topology Discovery Computers Computer Group and enable agent proxying for this server; after these steps are done, you should be fine.

Be sure to check Appendix A of the Exchange Management Pack guide when you run into trouble. This appendix gives you a lot of information on the script dependencies involved in the management pack. If there is a problem, this is a good place to start troubleshooting.

Troubleshooting SQL Server Management Packs

One of the most direct management packs we encounter is the SQL server. This is, in my opinion, also an essential management pack. The implementation process is pretty straightforward.

However, a few situations can cause the management pack to run into trouble. These are due mostly to off-default configurations of SQL server.

One of those settings that lead to problems is the situation where SQ uses a port other than the default (1433). In this situation the agent server is indicated as green

and the SQL server instance as yellow. To resolve this you need to create a network client alias. This means that you need to edit the SQL server. The following steps will create an alias on the SQL server:

1. Log on to the computer hosting the SQL Server 2000 default instance. If the server is monitored agentlessly, log on to the MOM management server that monitors the server.
2. Point to **Start**, **Programs**, **Microsoft SQL Server**, and then click **Client Network Utility**.
3. Click the **Alias** tab, and then click **Add**.
4. In the **Server alias** text box, enter the FQDN.
5. In the **Network libraries list** box, select **TCP/IP**.
6. In the **Connection parameters** box, clear the **Dynamically determine port** check box.
7. In the **Port number** text box, enter the port number used by the SQL Server 2000 default instance.
8. Click **OK**.
9. Click **Add** again to create an alias for the NetBIOS name.
10. In the **Server alias** text box, enter the NetBIOS name.
11. In the **Network libraries list** box, select **TCP/IP**.
12. In the **Connection parameters** box, clear the **Dynamically determine port** check box.
13. In the **Port number** text box, enter the port number used by the SQL Server 2000 default instance.

It is possible that the **SP_HelpDB** will not run correctly; this can be caused because the management pack is not able to determine the db-owner of the database. To work around the issue, change the dbowner role to a valid login; this can be done using the **sp_changedbowner**. Don't get all wild and do some research before changing the owner of the database to prevent downtime.

The last issue I would like to address is a problem with SQL-DMO (Data Management Objects) that uses a lot of memory monitoring large databases. Because the scripts are fired by the MOMHost.exe process, the memory consumption is added to the process. This will result in excessive memory usage of the MOM process, causing it to restart. This is a known issue, and cannot be resolved.

Troubleshooting Active Directory Management Packs

One of the most important management packs used in MOM is the Active Directory management pack. It not only checks for errors in AD but also monitors the replication performance and availability of Active Directory. All the available information about AD is gathered by several scripts, leaving a lot of things that can go wrong. Amazingly, there is little to no need to tweak the default installation after importing. They did a great job making this pack stable and easy to deploy.

After importing the management pack, a lot of problems can occur in the scripts that run on the domain controller. This happens mostly in environments that host multiple domain controllers (if your environment has only one domain controller, you probably have other problems besides MOM!). This is due to the use of NON visual basic or VBScript supported calls to IOOMADsInfo and IOOMADsInfo2. In case you run into problems with failed scripts on the servers, it can easily be resolved by installing the OOMADs that can be found in the *Support tools* directory in the MOM installation media.

Shortcuts…

IOOMADsInfo

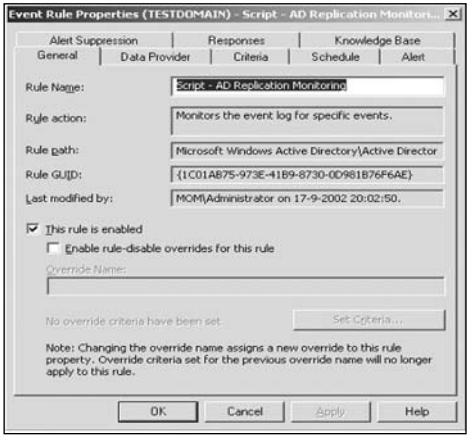
100MADsInfo is a class that is not automatically known in the VBScripting environment. Making calls to this class without having it will result in failures. Microsoft Active Directory management pack checks your Active directory roughly back and forth. This needs specialized calls. This object will supply these calls and make VBScript able to dig in. Installing the object helper should not be any problem with other classes.

If the domain controllers are involved in replication, the management pack may issue warnings about the replication time. This setting is changeable as a parameter in the Script - AD Replication Monitoring rule set of the Active Directory management pack. This rule is found in the following location (see Figure 13.9):

1. In the MOM 2005 Administrator console, double-click **Management Packs**.
2. Double-click **Rule Groups**.

3. Double-click **Microsoft Windows Active Directory**.
4. Double-click **Active Directory Windows 2000** and **Windows Server 2003**.
5. Double-click **Active Directory Availability**.
6. Double-click Script – AD Replication Monitoriing

Figure 13.9 Script - AD Replication Monitoring Rule

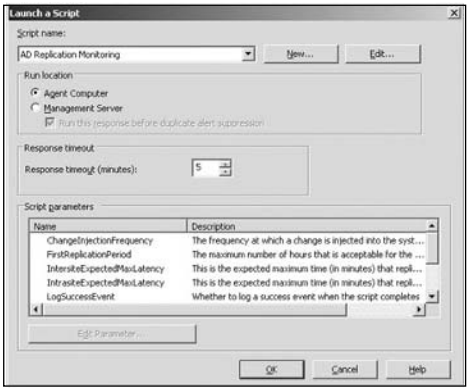


Next, go to the **Responses** tab to find the parameter (see Figure 13.10).

Figure 13.10 Script – AD Replication Monitoring Rule Responses Tab

On this screen you need to select the **AD Replication Monitoring** and select **Edit** to open the Launch a script dialog (see Figure 13.11).

Figure 13.11 Launching the AD Replication Monitoring Script



In the script parameters, locate and double-click the **IntersiteExpected MaxLatency** parameter. Change the default value of 15 minutes to the value you find acceptable for your site.

Backing Up and Restoring a MOM Server

MOM depends on a Microsoft SQL server instance for storage and collection of data. If you depend heavily on your MOM infrastructure, there can be a need to cluster this environment. This gives you the option to ensure availability on your MOM infrastructure, but it does not protect you from possible data corruption in your database. Therefore it is essential to make backups of the MOM database in a timely fashion. If the database fails and you do not have a backup from which to restore, you will likely need to start over from scratch.

Luckily, there are several ways to back up the database with or without the need of third-party software. In the context of this book we will address the backup and restore cycle as if there were no third-party software involved.

Best Practices According to Microsoft

- Always make a backup of the MOM database server and at least one management server. If there is a major failure you can restore the most important parts, like the MOM database and one of the management servers of the MOM infrastructure.
- You at least should make a full backup of the MOM database and one of the management servers on a daily basis. This way, you can quickly restore the environment. Microsoft recommends following the backup instructions shown in Table 13.1.

Table 13.1 Microsoft's Recommendations for Full and Incremental Backup of MOM Components

Item	Full Backup	Incremental Backup
MOM Database (OnePoint)	Daily	NA
MOM Reporting Database (SystemCenterReporting)	Monthly	Weekly
SQL Reporting Database (ReportServer)	Note 5	Note 5
Master Database (Master)	Note 1	Per your IT policies
Msdb Database (Msdbdata)	Note 2	Note 3
Management Packs and Reports (.akm and .xml files)	Note 4	NA
File Transfer files	As needed	NA

1. You should back up this database after installing and configuring the MOM database components and after making significant changes to logons or other security changes.

2. Only after first installing and configuring the MOM database components.

3. Only if you change the scheduled SQL Server Agent jobs that MOM uses.

4. You can do this monthly or after significant changes to management packs. You need to back up only the changed management packs.

5. You can do this on a recurring basis; frequency depends on how often reports change in your organization, or after significant changes to report definitions (additions, changes, and deletions).

6. Ref: http://www.microsoft.com/technet/prodtechnol/mom/mom2005/Library/c8557822-43b6-4f69-a8f5-5e7f65f48f00.mspx

Some Independent Advice

There is a lot to say about backup and restore. Too often, customer sites don't perform SQL backups regularly. We cannot stress this enough: a daily backup of the MOM operational database is absolutely essential. The time it takes to set up the backup (30 minutes) never comes close to the amount of time it takes to perform the complete installation of MOM, including the Agent rollout and management pack. One of the first things that need to be done after the installation of MOM is to set up the backup schedule. Just make a backup file of the database as described earlier in this chapter. Then back up the backup file to tape.

Shortcuts…

Management Pack Backup and Restore

When you use a test environment to create your own management packs, it is possible to use the backup and restore of management packs to transport the entire management pack to the production environment. When you build a management pack in your test environment, you can use the export function to make a backup of your custom management pack. This backup can then be restored in the live environment. Doing so will prevent configuration setting differences between the test and live environment, not to mention the time it saves.

Backing Up and Restoring the MOM Database

We'll now show you how to make a solid backup of your MOM Operational Data Database.

First, start SQL Server Enterprise Manager, expand a server group, and then expand a server (see Figure 13.12).

Expand **Databases**, right-click **Database**, point to **All Tasks**, and then click **Backup Database** (see Figure 13.13).

Figure 13.12 SQL Server Enterprise View

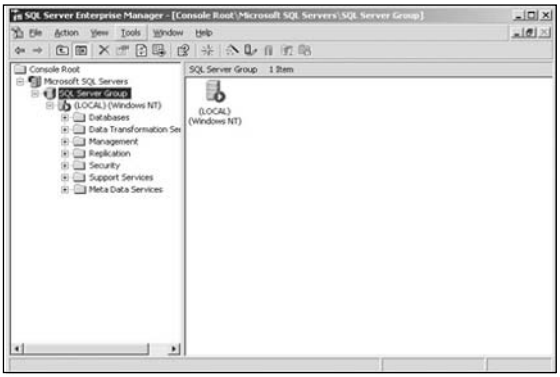
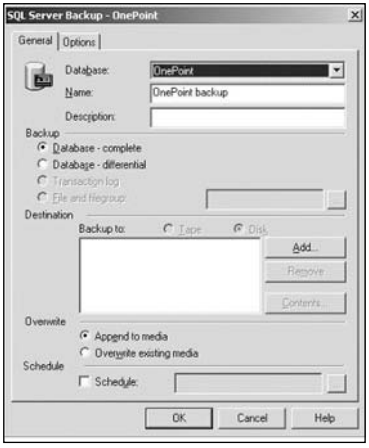


Figure 13.13 SQL Server Backup Job Dialog



In the **Name** box, type the backup set name. Optionally, type a description of the backup set in the **Description** box.

Under **Backup**, click **Database - complete**.

Under **Destination**, click **Tape** or **Disk**, and then specify a backup destination. If no backup destinations appear, click **Add** to add an existing destination or to create a new one.

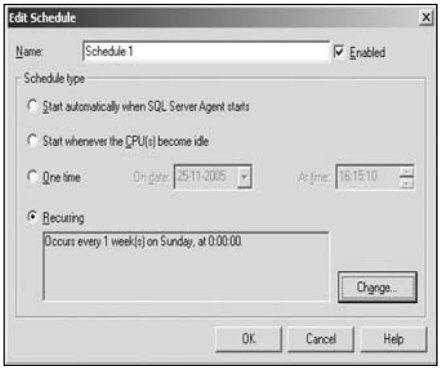
Under **Overwrite**, click one of the following options:

- **Append to media**, to append the backup to any existing backups on the backup device
- **Overwrite existing media**, to overwrite any existing backups on the backup device

Optionally, click to select the **Schedule** check box. You can then schedule the backup operation for a later time.

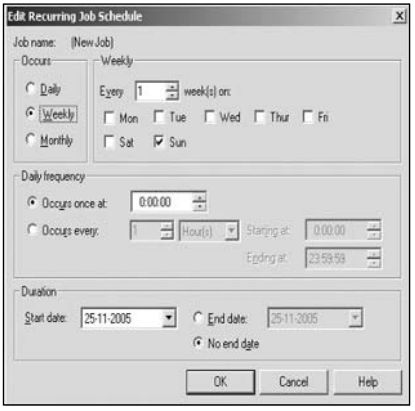
Select a time in the future to delay the start of the backup (see Figure 13.14).

Figure 13.14 Edit Schedule



If the schedule does not meet your requirements (it should not because you need to back up every day), you can use the **Change** button to edit the default schedule (see Figure 13.15).

Figure 13.15 Changing the Default Schedule

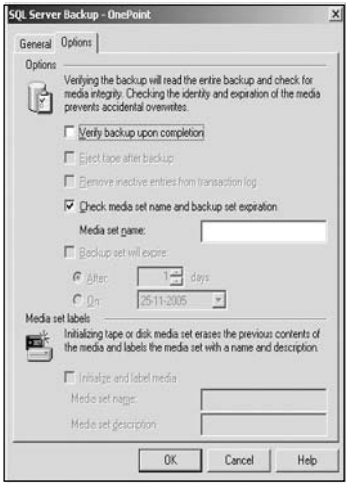


Optionally, click the **Options** tab, and then click to select one or more of the following check boxes (see Figure 13.16):

- **Verify backup upon completion** causes the backup to be verified at the end of the backup process.
- **Eject tape after backup** causes the tape to be ejected when the backup operation has completed. This feature is available only with tape devices.

- **Check media set name and backup set expiration** causes the backup media to be checked to prevent accidental overwrites. In the **Media set name** box, type the name of the media to be used for the backup operation. Leave this blank when you are specifying only the backup set expiration.

Figure 13.16 SQL Backup Job Options



After the backup jobs are running there is less to worry about. In case of a failure, depending on the scenario, there is more or less to restore. In case of a server crash, there is a restore of the server and all system databases, but if the MOM database is corrupted only one database restore should be necessary. In case the database is still on the server there should be no connection to the database, or the restore operation will fail. This means the MOM services on the management server need to be stopped. The next step is to take the database offline. You start by restoring the database backup file on a specified location. Now you're set to start with the restore operations database.

Select the **Databases** leaf next in the file menu and then select **Action -> Restore database**. This will start the Restore wizard, enabling you to restore (see Figure 13.17). If the database is not on the server you will not be able to select it from the drop-down box. In that case you need to type the name in the box. In the restore options, select **From device** and click on the **Select Devices…** button. This will open a selection dialog to select the device from which to restore (see Figure 13.18). Because backup devices need to be known by SQL server you probably need to select it from disk. Just click **Add**, browse to the file location, and select the file. Click **OK** until you return to the **Restore database** dialog. Then select the

Options tab (see Figure 13.19) and mark **Force over exiting database**; this will enable you to overwrite the existing database. Next click **OK** to start the restore process.

Figure 13.17 The SQL Restore Database Options

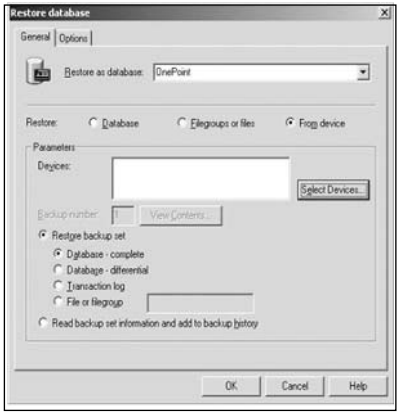


Figure 13.18 Choosing Restore Devices

The next step is to make sure the MOM Das account is able to write and read to and from the database. To check or set this access, follow these steps:

Using Enterprise Manager, select **Security**, and then select **Login** (see Figure 13.20).

Figure 13.19 SQL Restore Job Options Tab

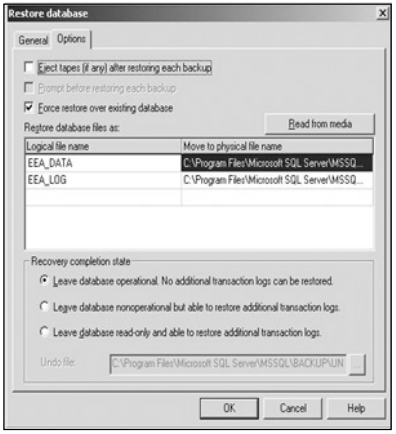
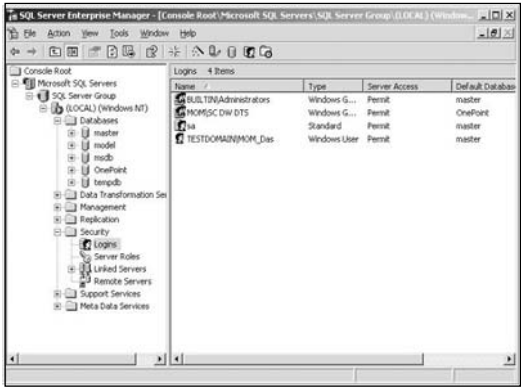


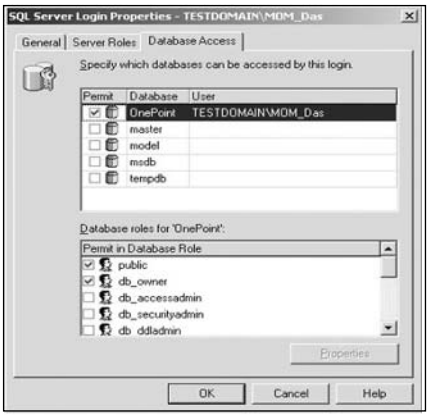
Figure 13.20 SQL Restore Setting Security after Restore, Select Login



Select **Das Account**, then right-click **Properties** (see Figure 13.21) and select **Database** (see Figure 13.22).

Figure 13.21 SQL Restore Setting Security after Restore, Select Das Account Properties

Figure 13.22 SQL Restore Setting Security after Restore, Select Das Database Access



Select **OnePoint**, and then select the checkbox for **db_owner**.

This will restore the entire database and configuration settings of your MOM environment.

Fire up the MOM management services and be prepared to receive the buffer space of data into the database.

Backing Up and Restoring Management Packs

Every time a new management pack is imported into the MOM management server, the old one is backed up to disk (default: %MOM install directory%\MPBackup\).

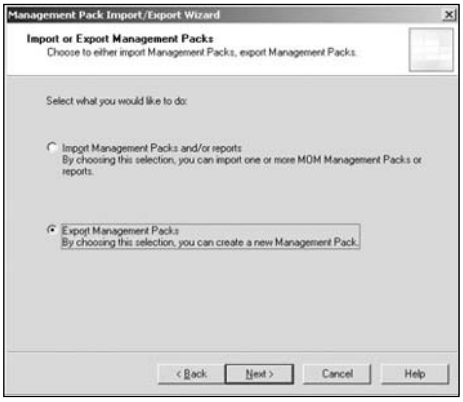
To back up your current management pack, maybe the one you customized, you can use two tools: the Import/Export Management Packs Wizard and ManagementModuleUtil.exe. Note the latter one is a command-line-driven tool.

For ease of use and overview of what the backup will contain, use the Import/Export Management Packs Wizard. This wizard offers a point-and-click interface instead of a command line. To make a correct backup of your custom management pack you need to know where the management pack is hidden in the MOM infrastructure. To start the wizard, select **Management Packs, Action, Import/Export management packs**. After that, a wizard will start that will welcome you (see Figure 13.23).

Figure 13.23 Import/Export Management Pack Wizard Welcome Screen

Of course, we're going to select **Next** and make sure we select **Export Management Packs** (see Figure 13.24) to be able to store the management pack information in an akm file. After selecting, click **Next**.

Figure 13.24 Import/Export Management Pack Wizard Select Export

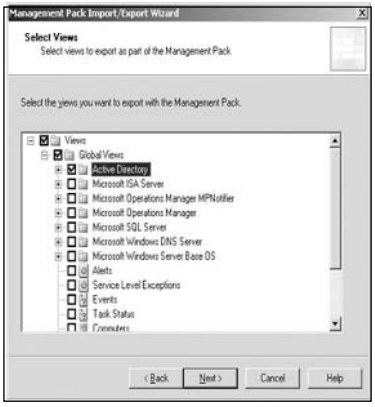


In this screen you're going to select the rule group that needs to be backed up. If you select a branch, the rules and folders underneath will be backed up. In the example you selected the Microsoft Windows Active Directory rule group (see Figure 13.25). It is not possible to make more than one selection. After you made your selection you can click **Next** to continue with the next page of the wizard.

Figure 13.25 Import/Export Management Pack Wizard Select Rule Group

Next, stop the views that need to be selected. These are Global views, the ones that are stored in the Public Views folder (see Figure 13.26). In this window you're able to select multiple views. For the sake of this example we suggest selecting the **Active Directory** node. After you're done selecting, click **Next** to go to the next selection dialog.

Figure 13.26 Import/Export Management Pack Wizard, Select Views



Next, stop the tasks that need to be backed up (see Figure 13.27); again, you need to select the tasks you want to take with your backup.

After selecting the tasks that need to be backed up, again click the **Next** button to continue. This brings us at the locations selection. This dialog (see Figure 13.28) offers several options to back up. Select the location where you want the backup and click **Next** to get to the summary page (see Figure 13.29) to start the backup. Click **Finish** to continue. This will back up all the selected information about the management packs you selected.

Figure 13.27 Import/Export Management Pack Wizard, Select Tasks

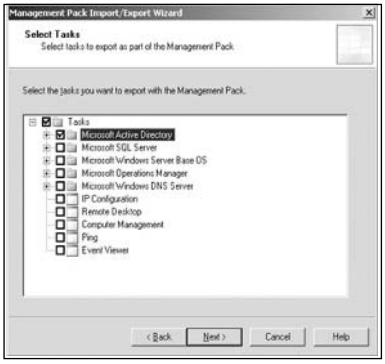


Figure 13.28 Import/Export Management Pack Wizard, Select Backup Location

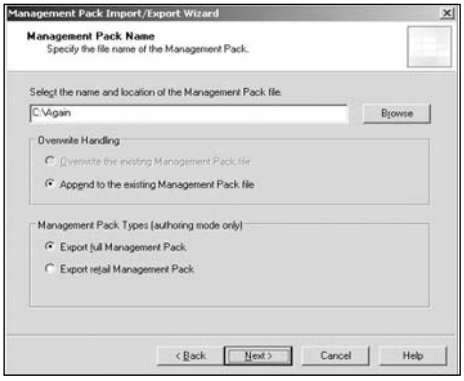
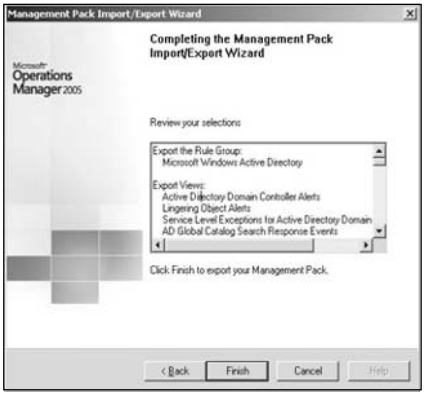


Figure 13.29 Import/Export Management Pack Wizard Completing



Summary

In this chapter we've taken a look at the low-level tools from the resource kit, available to MOM for your comfort and advance maintenance. These tools come in handy when troubleshooting a failed MOM infrastructure. However, the most probable cause of errors is not in the Agents but in the server and the management pack rules. We addressed some common issues that often go wrong and that will save you a lot of time if addressed first. We also addressed backing up and restoring the MOM infrastructure and why it is essential.

Solutions Fast Track

Using the MOM Resource Kit

- ☑ Cleanup MOM removes installations of agents and other MOM-related services in a management server. This is a brute-force removal tool.
- ☑ Management Group Utility enables you to view the management group configuration and check for corrupted configurations.
- ☑ MOM Information Utility enables you to compare the rule sets on the agent with the server. Also, it enables you to place the offline agent in maintenance mode.
- ☑ Finally, use the MOM Inventory tool to gather all information of the MOM installation. This can be very handy if Microsoft Professional Support Services (MPSS) asks for it.

Troubleshooting Management Packs

- ☑ The Active Directory Management Pack needs to have some time to settle. This is due to the discovery scripts that can have an interval of up to 24 hours. During this time scripts that need information from this script as input will fail.
- ☑ If you're in a multidomain environment, there is a possibility that the servers fail on a script. This can be overcome with installing the IOOMADsinfo and IOOMADsinfo2 objects.
- ☑ To time the replication you need to tweak the I**ntersiteExpectedMaxLatency** parameter.

Backing Up and Restoring a MOM Server

- ☑ Back up your MOM database server… always.
- ☑ Restoring the operational database will restore all configuration settings.
- ☑ You can back up management packs by exporting them to file (*.akm).
- ☑ You can restore them by reimporting them.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: I have a virus scanner. Is there any way I can make a management pack for this on my own?

A: Yes. In the MOM resource kit there is a tool called MPWizard that enables you to create new management packs from scratch. Just run the MPWizard on the machine where the application resides.

Q: Somehow our MOM server has stopped displaying new alerts. What's wrong?

A: There can be a lot of things that cause these symptoms. The first thing you need to check is the MOM Server Queue Size Space Percent Used performance counter. If there is a problem connecting to the database this performance counter displays a value at or close to 100%. In that case you need to sort out what is preventing the connection to the database. If that is not the issue, try the MOM Resource Kit tool Eventcreator to simulate the events.

Q: How many agents can be installed on one server?

A: There can be only one agent service installed on a server. However, that agent can report to a max total of four management groups (this is also known as a multihomed agent). The agent will process the rules of the management group separate from the other management groups and will manage separate MOM queues for every management group.

Q: What is the course of action if I have more than two or more management servers in one management group and one of them died?

A: All automatically installed agents will fail over to the other management server. The agents that are installed manually (like the ones behind the firewall) don't fail over to another server automatically if not set on installation time. If the server is back online the agents will fail back automatically.

Q: I try to install an agent behind a firewall but it does not show up in the operator console. Why not?

A: This can be due to several issues. The first one is the fact that MOM uses a port above the well-known port list, TCP port 1270. This should be so that open traffic can pass. If you're running ISA Server 2004, there is a System Rule that gives access on all needed ports.

It is possible that the MOM server is set to reject manually installed agents. If this is the case you need to check whether the server you want to monitor is discovered. If this is the case, follow these steps:

1. Deselect **Reject manual installed agents**.
2. Delete the selected computer from the unmanaged computer list.
3. Restart the MOM servers on the server.

After doing so the server will show up in the **Pending actions**. Select **Accept** to start monitoring.

Appendix A

Microsoft MOM Management Packs

Solutions in this appendix:

- **Microsoft Management Packs**
- **Third-Party Hardware Management Packs**
- **Third-Party Software Management Packs**

Introduction

This appendix is intended to provide additional information regarding management packs available from Microsoft and third-party vendors that, in the interest of time, were not covered in this book. It is broken down into three sections:

- **Microsoft Management Packs** Management packs developed and distributed by Microsoft for management and monitoring of their products.
- **Third-Party Hardware Management Packs** Management packs developed and distributed by third-party vendors for managing and monitoring hardware with MOM 2000/2005. Some of these are written by the manufacturer, some are not.
- **Third-Party Software Management Packs** Management packs developed and distributed by third-party vendors for managing and monitoring software with MOM 2000/2005. Some of these are written by the manufacturer; some are not.

Microsoft Management Packs

This section addresses management packs that are intended for management and monitoring of core OS and Active Directory functions that were not previously covered in this book. Table A.1 lists the name of the management pack and a brief description.

Additional Active Directory and Windows Management Packs

Table A.1 Additional Active Directory and Windows Management Packs

Management Pack Name	Management Pack Description
Internet Information Services (IIS)	Monitors IIS services, performance, broken links, and unavailable sites. Also reports on IIS security breaches.
Microsoft Web Sites and Services	A very cool management pack. It continually checks the availability and performance of Web sites, regardless of the underlying Web service (IIS, Apache, etc.).

Continued

Table A.1 continued Additional Active Directory and Windows Management Packs

Management Pack Name	Management Pack Description
Network Load Balancing (NLB)	Used to monitor Windows 2000 and Windows 2003 clusters.
Windows Desktop Base OS	Used to manage and monitor Windows XP desktops. Its use should be limited, since it still requires a MOM license.
Windows NT 4.0	Monitors legacy Windows NT 4.0 systems. Very limited monitoring capabilities.
Windows System Resource Manager	A very powerful management pack. Used exclusively with Windows Enterprise and Datacenter editions. WSRM handles the allocation of system resources based on business need. The WSRM management pack monitors many aspects of WSRM, including service outages, application exceptions, and accounting volume disk space.
Windows Terminal Server	A great addition to any MOM system. Includes many different management views and reports relating specifically to the health of the Windows Terminal Server service.

Additional Microsoft Products Management Packs

Table A.2 outlines a variety of management packs available for managing and monitoring additional Microsoft products. For information on management packs relating to Microsoft Exchange and Microsoft SQL, see Chapters 6 and 7, respectively. Keep in mind that this is only a partial list, and there are many more management packs available on Microsoft's Web site. To find out more, visit www.microsoft.com/management/mma/catalog.aspx.

Table A.2 Additional Microsoft Product Management Packs

Management Pack Name	Management Pack Description
BizTalk Server (2002/2004)	Separate management packs, one for 2003 and one for 2004. These management packs monitor events that are generated in the server's Application log by the BizTalk service.
Commerce Server	This management pack monitors events generated by Commerce Server 2000, which are placed in the application and system event logs.
Internet Security and Acceleration Server 2000/2004	Monitors and manages ISA Server 2000 and 2004. Additional configuration on the ISA is required in order for MOM to be able to manage and monitor. Read the release notes that come with the management pack before configuring.
Office Live Communications Server 2005	There are multiple management packs available for Office Live Communication Server 2005. Make sure that you use the management pack that corresponds with the service pack version of your OLCS 2005 system.
Project Server 2003	Monitors the event logs of a server running Project Server 2003. Reports on issues such as database connectivity problems, failed/stopped services, and other Project Server-related functions.
Virtual Server	Monitors availability and performance of Microsoft Virtual Server 2005. Being virtual-aware allows this management pack to address issues not typical of physical servers. The management pack also allows for starting, stopping, and restarting of Virtual Servers. The Virtual Server management pack also allows for agentless monitoring.
Windows Rights Management	Manages WRM, notifying MOM of service outages and potential configuration problems.

Third-Party Hardware Management Packs

The following section outlines some of the third-party (non-Microsoft developed) management packs available for the management of hardware devices. For your convenience, many of these third-party hardware management packs come with a free 30-day trial. We suggest trying these in a lab environment whenever possible because neither Microsoft nor the hardware manufacturer directly supports them.

IBM Management Packs

Table A.3 lists three third-party management packs for IBM hardware.

Table A.3 Third-Party Management Packs for IBM Hardware

Management Pack Name	Management Pack Description	Third-Party Developer
Virtual Agent for IBM ESS Storage	Offers management and monitoring support for IBM's Enterprise Storage Server.	eXc Software
Virtual Agent for IBM BladeCenter	Offers support for all SNMP-ready IBM BladeCenter products.	eXc Software
Virtual Agent for IBM FAStT Storage	Monitor's IBM's TotalStorage DS4000-series (formerly called FAStT) line of disk storage products.	eXc Software

BlackBerry Management Packs

Table A.4 lists two third-party management packs for BlackBerry handheld devices from Research In Motion.

Table A.4 Third-Party Management Packs for BlackBerry Handheld Devices

Management Pack Name	Management Pack Description	Third-Party Developer
BlackBerry Enterprise Server	This service pack is provided for monitoring and management of BlackBerry Enterprise Server (BES) 4.0 and later, as well as BlackBerry handheld devices. Has the ability to manage licenses, monitor the BES database, as well as utilization statistics.	iVision
Virtual Agent for BlackBerry	Similar features as the preceding management pack; however, this third-party management pack can manage both BES 3.0 and BES 4.0.	eXc Software

Additional Hardware Management Packs

Additional third-party management packs are listed in Table A.5.

Table A.5 Additional Hardware Management Packs

Management Pack Name	Management Pack Description	Third-Party Developer
Virtual Agent for 3Com	Provides for monitoring and management of a variety of 3Com hardware devices via SNMP.	eXc Software
eXc Software APC	Provides for monitoring and management of all APC products via SNMP. Can monitor status of APC electrical ports.	eXc Software
SMP – APC UPS	Monitors APC indicators including battery status, power information, and current UPS status.	JalaSoft

Third-Party Software Management Packs

The following section outlines some of the third-party (non-Microsoft developed) management packs available for the management of software applications (see Table A.6). For your convenience, many of these third-party software management packs come with a free 30-day trial. We suggest trying these in a lab environment whenever possible because they are not directly supported by Microsoft, and in some cases, the software developer.

Table A.6 Additional Software Management Packs

Management Pack Name	Management Pack Description	Third-Party Developer
Citrix Metaframe XP Management Pack	Provides for management and monitoring of Citrix XP Enterprise Edition presentation servers.	Citrix
DNSAnalyzer	Used to analyze a variety of DNS applications, including Microsoft's DNS, BIND, and QIP.	NetPro
Veritas Backup Exec	Used to filter events generated by Veritas Backup Exec for purposes of notifying IT staff of required actions.	Veritas
Virtual Agent for Check Point Firewall	This can either fall in the hardware or software category. Supports monitoring and management of Check Point firewall, and all Check Point Firewall-enabled Nokia appliances.	eXc Software
Virtual Agent for Macintosh OS X	A fantastic management pack for users with a high Macintosh population. This management pack can monitor CPU usage (total and per process), disk utilization, and process state.	eXc Software
Virtual Agent for McAfee	Used for management and monitoring of McAfee anti-virus servers using SNMP. Monitors alerts generated from traps created by a McAfee AV server.	eXc Software

Continued

Table A.6 continued Additional Software Management Packs

Management Pack Name	Management Pack Description	Third-Party Developer
Virtual Agent for Novell	Uses SNMP for monitoring and management of Novell servers.	eXc Software
Virtual Agent for TrendMicro	Similar to the McAfee virtual agent. Uses SNMP for monitoring and management of TrendMicro Anti-virus servers.	eXc Software
Virtual Agent for VMware	Similar in concept to the management pack made by Microsoft to their Virtual Server. This management pack can monitor and manage virtual hardware utilization (CPU, memory, disk, etc.) via SNMP. Offers support for VMware Workstation, GSX, and ESX editions.	eXc Software

Index

Numbers

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

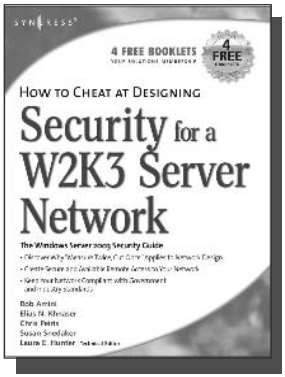
V

W

X

Syngress: *The Definition of a Serious Security Library*

Syn•gress (sin-gres): *noun*, *sing*. Freedom from risk or danger; safety. See *security*.



AVAILABLE NOW
order @
www.syngress.com

How to Cheat at Designing Security for a Windows Server 2003 Network

Neil Ruston, Chris Peiris

The next book in our best selling and critically acclaimed How to Cheat series. While considering the security needs of your organiztion, you need to balance the human and the technical in order to create the best security design for your organization. Securing a Windows Server 2003 enterprise network is hardly a small undertaking, but it becomes quite manageable if you approach it in an organized and systematic way. This includes configuring software, services, and protocols to meet an organization's security needs.

ISBN: 1-59749-243-4

Price: $39.95 US $55.95 CAN

How to Cheat at IT Project Management

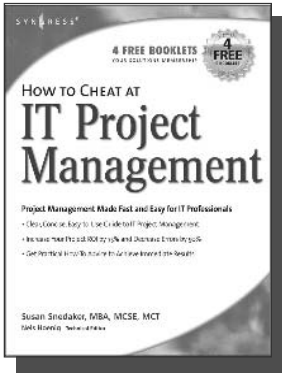
AVAILABLE NOW
order @
www.syngress.com

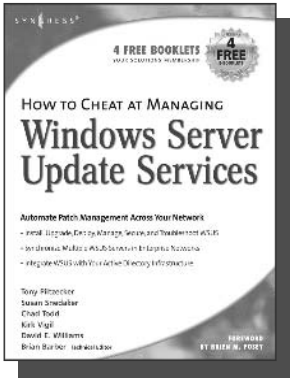
Susan Snedaker

Most IT projects fail to deliver – on average, all IT projects run over schedule by 82%, run over cost by 43% and deliver only 52% of the desired functionality. Pretty dismal statistics. Using the proven methods in this book, every IT project you work on from here on out will have a much higher likelihood of being on time, on budget and higher quality. This book provides clear, concise, information and hands-on training to give you immediate results. And, the companion Web site provides dozens of templates for managing IT projects.

ISBN: 1-59749-037-7

Price: $44.95 US $62.95 CAN





AVAILABLE NOW
order @
www.syngress.com

How to Cheat at Managing Windows Server Update Services

Brian Barber

If you manage a Microsoft Windows network, you probably find yourself overwhelmed at times by the sheer volume of updates and patches released by Microsoft for their products. You know these updates are critical to keep your network running efficiently and securely, but staying current amidst all of your other responsibilities can be almost impossible. Microsoft's recently released Windows Server Update Services (WSUS) is designed to streamline this process. Learn how to take full advantage of WSUS using Syngress' proven "How to Cheat" methodology which gives you everything you need and nothing you don't.

ISBN: 1-59749-027-X

Price: $39.95 U.S. $55.95 CAN

Syngress: *The Definition of a Serious Security Library*

Syn•gress (sin-gres): *noun*, *sing*. Freedom from risk or danger; safety. See *security*.

AVAILABLE NOW
order @
www.syngress.com

How to Cheat at Managing Windows Small Business Server 2003

Susan Snedaker, Daniel H. Bendell (Technical Editor)

If running a Windows Small Business Server 2003 network is just one of your many job responsibilities, this book is for you. It applies the tried and true "80/20" rule to this incredibly complex operating system, providing you with exactly the information you need to install, configure, and troubleshoot the W2K3 features most likely to ruin your day (such as setting user permissions, restoring lost data, and sharing hardware) without having to wade through material you don't need.

ISBN: 1-93226-680-1

Price: $49.95 US $72.95 CAN

How to Cheat Designing Windows Server 2003 Active Directory

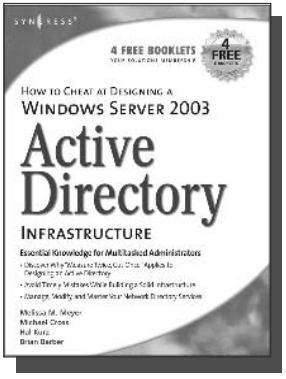
AVAILABLE NOW
order @
www.syngress.com

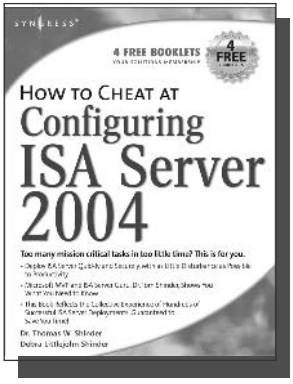
Melissa Craft, Michael Cross, Hal Kurz, Brian Barber

This book will start off by teaching readers to create the conceptual design of their Active Directory infrastructure by gathering and analyzing business and technical requirements. Next, readers will create the logical design for an Active Directory infrastructure. Here the book starts to drill deeper and focus on aspects such as group policy design. Finally, readers will learn to create the physical design for an active directory and network Infrastructure including DNS server placement; DC and GC placements and Flexible Single Master Operations (FSMO) role placement.

ISBN: 1-59749-058-X

Price: $39.95 US $55.95 CAN





COMING SOON!
order @
www.syngress.com

How to Cheat at Configuring ISA Server 2004

Dr. Thomas W. Shinder, Debra Littlejohn Shinder

If deploying and managing ISA Server 2004 is just one of a hundred responsibilities you have as a System Administrator, "How to Cheat at Configuring ISA Server 2004" is the perfect book for you. Written by Microsoft MVP Dr. Tom Shinder, this is a concise, accurate, enterprise tested method for the successful deployment of ISA Server. .

ISBN: 1-59749-057-1

Price: $34.95 U.S. $55.95 CAN

Syngress: *The Definition of a Serious Security Library*

Syn•gress (sin-gres): *noun, sing.* Freedom from risk or danger; safety. See *security*.

AVAILABLE NOW
order @
www.syngress.com

The Best Damn Windows Server 2003 Book Period

Susan Snedaker

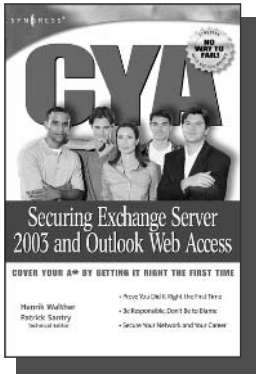
Windows Server 2003 is certainly Microsoft's most robust, and complex, enterprise operating system developed to date. Any one of the component "services" in Server 2003 has more features and functionality than existed in the entire Windows NT 4 operating system! In addition, the audience of System Administrators has now evolved to a highly professional, skills certified community of IT professionals with a need for the tens of thousands of pages of Microsoft documentation and web-based support to be distilled into a concise, applied format. This is the book that meets the needs of today's Windows Server 2003 professional.

ISBN: 1-93183-612-4

Price: $59.95 US $79.95 CAN

CYA Securing Exchange Server 2003 & Outlook Web Access

AVAILABLE NOW
order @
www.syngress.com



Henrik Walther, Patrick Santry

A highly portable, easily digestible road-map to configuring, maintaining and troubleshooting essential Exchange Server 2003 features, assuring that the reader has in fact covered their a**. The book is organized around the 11 Microsoft Management Consoles that contain the configuration menus for the essential features. The options within each menu are explained clearly, potential problems are identified up-front, and configurations are subsequently presented in the aptly named "By the Book" section for that MMC. Readers will also appreciate the "Reality Check" sidebars throughout, which present valuable cost/benefit analyses of situations where there is no single "right" answer.

ISBN: 1-93183-624-8

Price: $39.95 US $59.95 CAN

AVAILABLE NOW
order @
www.syngress.com

Microsoft Log Parser Toolkit

Gabriele Giuseppini and Mark Burnett

Do you want to find Brute Force Attacks against your Exchange Server? Would you like to know who is spamming you? Do you need to monitor the performance of your IIS Server? Are there intruders out there you would like to find? Would you like to build user logon reports from your Windows Server? Would you like working scripts to automate all of these tasks and many more for you? If so, "Microsoft Log Parser Toolkit" is the book for you...

ISBN: 1-93226-652-6

Price: $39.95 U.S. $57.95 CAN