Kerrie Meyler
Cameron Fuller

with Chris Amaris, John Joyner, Alec Minty

With A Preview of **Operations Manager 2007**

Microsoft® Operations Manager 2005

Kerrie Meyler
Cameron Fuller

with Chris Amaris, John Joyner, and Alec Minty

Microsoft® Operations Manager 2005

UNLEASHED

SAMS | 800 East 96th Street, Indianapolis, Indiana 46240 USA

Microsoft Operations Manager 2005 Unleashed

International Standard Book Number: 0-672-32928-X

Library of Congress Catalog Card Number: 2006027379

Printed in the United States of America

First Printing: November 2006

09 08 07 06 4 3 2 1

Trademarks

Warning and Disclaimer

Bulk Sales

Sams Publishing offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales
1-800-382-3419
corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact

International Sales
international@pearsoned.com

This Book Is Safari Enabled

The Safari® Enabled icon on the cover of your favorite technology book means the book is available through Safari Bookshelf. When you buy this book, you get free access to the online edition for 45 days.

Safari Bookshelf is an electronic reference library that lets you easily search thousands of technical books, find code samples, download chapters, and access technical information whenever and wherever you need it.

To gain 45-day Safari Enabled access to this book:

- Go to http://www.samspublishing.com/safarienabled
- Complete the brief registration form
- Enter the coupon code TAK5-68KJ-SEPT-3VJ2-7S21

If you have difficulty registering on Safari Bookshelf or accessing the online edition, please e-mail customer-service@safaribooksonline.com.

Acquisitions Editor
Neil Rowe

Managing Editor
Gina Kanouse

Project Editor
Lori Lyons

Copy Editor
Geneil Breeze

Proofreader
Paula Lowell

Technical Editors
Brett Bennett
John Joyner
Kevin Saye

Publishing Coordinator
Cindy Teeters

Multimedia Developer
Dan Scherf

Book Designer
Gary Adair

Page Layout
Nonie Ratcliff
Bronkella Publishing

Contents at a Glance

Table of Contents

About the Authors

Kerrie Meyler, MA, BA, MCSE, CNA, is an independent consultant and former trainer with more than 15 years' experience in IT. While at Microsoft in Field Technical Sales for four years she focused on infrastructure and management, presenting at numerous product launches. She also presented at internal Microsoft conferences and received company recognition and awards including a SPAR MGS award. An MCT for six years, Kerrie worked with Microsoft Learning to develop functional specifications for the 2550: Implementing Microsoft Operations Manager 2000 Microsoft Official Curriculum course and did the beta teach for that course. She also participated in the alpha walkthrough for the 2274: Managing a Microsoft Windows Server 2003 Environment course. As an author, she coauthored an IIS 6.0 Administration book.

Cameron Fuller, BS, MCSE, is a Senior Lead consultant for Catapult Systems, an IT consulting company and Microsoft Gold Certified Partner in Advanced Infrastructure Solutions. He focuses on management solutions, and serves as the Microsoft Operations Management Champion for Catapult. Cameron's 15 years of infrastructure experience include working with medium to large companies in the retail, education, healthcare, distribution, transportation, and energy industries. Cameron continually focuses on improving his existing business and technical skill sets through hands-on experience and leveraging certifications including an MCSE since NT 3.51, MCSA, A+, Linux+, Server+, and CCSA. Cameron is also a public speaker, co-presenting with Microsoft on MOM 2005 at TechEd and the MOM 2005 product launches in Dallas and Tulsa.

Contributors:

Chris Amaris is chief technology officer and cofounder of Convergent Computing. He has more than 20 years of consulting experience and specializes in security, performance tuning, systems management, migration, and messaging. A prolific book-publishing veteran, Chris has written on Network Security, Windows 2000 Performance Tuning, Windows 2000 Security, Windows Server 2003, and Exchange Server 2003. His certifications include Certified Information Systems Security Professional (CISSP), Certified Homeland Security (CHS III), MCSE, Novell CNE, Banyan CBE, and Certified Project Manager.

John Joyner, LCDR USN-R, BS, MCSE, is a highly decorated U.S. Navy computer scientist, designing and operating the U.S. Navy's first Internet-connected aircraft carrier network. Today he is a chief architect at ClearPointe, a Microsoft Gold Certified Partner for Advanced Infrastructure and Security Solutions and a pioneer in the managed service provider industry. John has designed MOM deployments for some of the world's largest companies, and also is the creator of ClearPointe's hosted NOC solution, awarded the Central Region Partner of the Year Competency award at the Microsoft 2006 Worldwide Partner Conference.

Alec Minty is a Senior Consultant with Convergent Computing. Alec is a longtime advocate of operations management, systems management, and security technologies. He specializes in designing, implementing, and supporting MOM and SMS infrastructures for a variety of large utility, telecommunications, and engineering organizations. Alec also has experience in the deployment, migration, and integration of other technologies such as Windows, Exchange, Active Directory, ISA, identity management, and SQL Server. He is a contributing author on *ISA 2004 Unleashed*.

Dedication

To our spouses, Stan and Beth. This book would not have come about without your infinite understanding and support. We owe you deeply for your endless patience and tolerance as we labored over "the book" and even brought our laptops with us when we were supposed to be on vacation.

—Kerrie Meyler and Cameron Fuller

Acknowledgments

Many people have helped bring this book to fruition, and we would like to thank the considerable number of folks who helped with this project. This includes Chris Amaris, John Joyner, and Alec Minty for their contributions to the book; Jason Leznek for cheerleading and inspiration; Stan Liebowitz, Clint Tate, David D'Entremont, Rory McCaw, Byron Holt, and John Arnott; Sripriya Sundararaman for helping with the "PingPack"; Anser Siddiqui and David Womack for their assistance with the MOM database monitoring management pack; and John Savill, David Minchew, and Zach Smith; and www.gotdotnet.com for use of the MOM Agent Monitor.

We would also like to thank Geniant Consulting of Dallas (Cameron's former employer), for its focus on well-built and managed infrastructure foundations and support of the countless hours that Cameron spent writing this book. Additional thanks are due to our reviewers: Brett Bennett, John Joyner, Kevin Saye; the Microsoft MOM Team including Dale Koetke, (and alphabetically) Gerardo Dilillo, Kevin Holman, Glen Houghton, Justin Incarnato, Vlad Joanovic, Lorenzo Rizzi, Tom Theiner, and Travis Wright. Thanks also to our editorial and publishing staff including Elizabeth Peterson, Kristin Weinberger, Jana Jones, Neil Rowe, Curt Johnson, Jake McFarland, Lori Lyons, and Nonie Ratcliff.

Finally, we thank Kerrie's friends and former coworkers at Microsoft, including Matt Hester, Ron Grattopp, Steve Roach, Greg Lirette, Aimee Lirette, Sean Kelly, Brian Moore, Regina Rafraf, Steven DeSalvo, and Dave Meltzer: Thank you for just being there!

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

You can email or write me directly to let me know what you did or didn't like about this book—as well as what we can do to make our books stronger.

Please note that I cannot help you with technical problems related to the topic of this book, and that due to the high volume of mail I receive, I might not be able to reply to every message.

When you write, please be sure to include this book's title and author as well as your name and phone or email address. I will carefully review your comments and share them with the author and editors who worked on the book.

E-mail: opensource@samspublishing.com

Mail: Karen Gettman
Editor-in-Chief
Sams Publishing
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at www.samspublishing.com/register for convenient access to any updates, downloads, or errata that might be available for this book.

Introduction

With the licensing of NetIQ's Operation Manager technology in 2000, Microsoft sent a message that it was serious about server monitoring and management. This message was well received; those production environments running Windows servers and using a Microsoft infrastructure require tools to help them be proactive in managing those servers and the applications and services within.

However, operations management is more than just looking at individual event logs from hundreds or even thousands of servers. It's about co-relating what may appear to be unrelated events across servers and determining what information is significant and what is not, what may portend a potential problem, and then taking available vendor and in-house knowledge and using that as a base of information in both preventing problems and solving them.

Operations management is not just a software application; successfully maintaining Service Level Agreements involves people, tools, and processes. Although Microsoft Operations Manager (MOM) is a tool, it is not a piece of software that you can simply install and have instantly working. A successful implementation of MOM involves planning, design, and an understanding of how to utilize its management packs. Operations management tools also have several target groups of users: computer operations, help desk personnel, and administrators of various areas, including operating systems, security, database, messaging, and web servers, to name a few.

This book intends to answer the perennial question: "Now that I've run Setup, how do I make this work?" Successfully implementing operations management takes planning and design. Successful administration and use of MOM requires managing the thousands of rules it can encompass, working with the various types of administrators, and keeping management informed of trends.

We do have a disclaimer: Resources and management packs related to MOM 2005 change rapidly. Sometimes it seemed that as soon as we completed a chapter, the information was already outdated. The information in this book is current as of the time it was written, and the authors have done their best to keep up with the constant barrage of changing management packs, MOM-related utilities, URLs, and knowledge base articles.

Part I: Operations Management Overview and Concepts

Part I introduces the reader to MOM 2005, outlining its features and functionality and comparing and contrasting it to MOM 2000 and MOM 2005 Workgroup Edition. Chapter 1, "Operations Management Basics," discusses the concepts behind operations management and Microsoft's management approach, and introduces MOM and Microsoft's management suite of products. An overview of ITIL and MOF is included along with a

discussion of how the different MOF quadrants relate to MOM. In Chapter 2, "What's New," we cover the history of MOM and compare MOM 2005 with MOM 2000 and the 2005 Workgroup Edition. Chapter 3, "How Does It Work?," appropriately gives an architectural overview and discusses the MOM components.

Part II: Planning and Installation

Before diving into MOM's setup program, it is best to take a step back to map out the requirements for your management environment and planning your server topology. Chapter 4, "Planning Your MOM Deployment," discusses the steps required to successfully plan a MOM installation. Chapter 5, "Planning Complex Configurations," addresses more advanced implementations including planning for redundancy and how to architect management groups. In Chapter 6, "Installing MOM 2005," we discuss hardware and software requirements before going through the steps to install the various server components in a management group using a "simple" configuration. (We talk about more complex configurations in Part III.) Chapter 7, "Upgrading to MOM 2005," discusses the required steps to upgrade from MOM 2000 or MOM 2005 Workgroup Edition. The complexity of your upgrade is related to the complexity of your MOM 2000 deployment.

Part III: Deploying MOM

With MOM 2005 installed, how do you start using it? Chapter 8, "Post-Installation Tasks," discusses what you need to know to get started with MOM. We discuss basic configuration and administration of MOM and MOM Reporting, include an overview of the MOM consoles, and drill down into the Administrator and Operator consoles. Chapter 9, "Installing and Configuring Agents," goes through the details of computer discovery, implementing agents, and potential problems related to agent installation. Chapter 10, "Complex and High Performance Configurations," discusses various management server and management group configurations, implementing redundant components, and architecting for high performance. In Chapter 11, "Securing MOM," we discuss the different security groups MOM 2005 uses, user and service accounts MOM utilizes, firewall considerations, configuring MOM to monitor workgroups and nontrusted domains, and communications security.

Part IV: Administering MOM

All applications require administration, and MOM is no exception. Chapter 12, "Backup and Recovery," discusses the different components required in a complete backup and recovery plan, and how to design a disaster recovery plan. Chapter 13, "Administering Management Packs," covers the components of a management pack; how to troubleshoot, deploy, and manage management packs; and the details of importing and exporting management packs and reports into your MOM environment. Chapter 14, "Monitoring with MOM," discusses the different rule types in MOM and their components, and approaches for tuning rules.

Part V: Managing with MOM

In this section of the book we get into what MOM is really about—using it to ease the pain of monitoring and managing your systems and applications. We discuss using MOM to manage different aspects of your environment: the operating system and Windows Server components (Chapter 15, "Managing the Operating System"); Active Directory (Chapter 16, "Managing Directory Services"); Exchange Server (Chapter 17, "Managing Microsoft Messaging"); and SQL Server (Chapter 18, "Database Management"). These chapters talk about the issues faced by administrators in each of these areas and how MOM 2005, with its management packs, can help you monitor operational issues and maintain stability and your SLAs (Service Level Agreements).

Part VI: Moving Beyond MOM 2005

We now look at extending one's use of MOM 2005 with connectors, third-party management packs and customization, and at Microsoft's direction for operations management. In Chapter 19, "Interoperability," we cover the role of product connectors in communicating with other management systems and third-party enterprise consoles. The chapter also focuses on using management packs to monitor hardware, other operating systems, and network components, and concludes with an introduction to Microsoft's solution accelerators for MOM. Chapter 20, "Developing Management Packs," Chapter 21, "Using and Developing Reports," and Chapter 22, "Using and Developing Scripts," discuss the process of customizing MOM with management packs—several of which we include for your own use, reports, and scripts. Chapter 23, "Touring Operations Manager 2007," presents a high-level view of where Microsoft is going with the next version of the product, looking at System Center Operations Manager 2007 at the time of its Beta 2 test release.

Appendixes

This book contains six appendixes:

- Appendix A, "MOM Internals," contains information on MOM architecture including processing flow and the queue files.
- Appendix B, "Registry Settings," discusses some of the more significant registry settings used by MOM 2005.
- Appendix C, "Performance Counters," discusses the performance counters specific to MOM.
- Appendix D, "Database Views," describes available views for the operations and reporting databases.
- Appendix E, "Reference URLs," provides references for and descriptions of many URLs that are helpful for MOM administrators.
- Appendix F, "On the CD," describes the content included with the CD, which includes the Reference URLs as live links and a number of management packs we developed and reference in the book.

About the CD-ROM

This book includes a CD-ROM containing scripts, examples, and our own management packs referred to throughout the book. It also includes live links from Appendix E to save you the trouble of having to type in what sometimes are lengthy URLs. The MOM 2005 Resource Kit is also on the CD. Refer to Appendix F for more information.

Who Should Read This Book

This book is targeted for the systems professional who wants to be proactive in managing the operational environment. This audience is cross-industry, ranging from a single system administrator in a smaller organization to larger businesses where multiple individuals are responsible for the operational health of the operating system and the subsystems running within it. By providing insight into MOM's capabilities and tools to help with a successful implementation, the book hopes to enable a more widespread understanding and use of Microsoft Operations Manager.

PART I

Operations Management Overview and Concepts

IN THIS PART

This page intentionally left blank

CHAPTER 1

Operations Management Basics

IN THIS CHAPTER

Welcome to Microsoft Operations Manager 2005—one of the most useful and exciting products for anyone responsible for managing servers and applications in the Windows environment. Microsoft Operations Manager (MOM) is a management tool that consolidates information about your Windows servers while administering them from a centralized location. MOM gives you the tools you need to get and stay in control of your Windows environment and helps in managing, tuning, and securing Windows 2000, Windows Server 2003, and Windows-based applications. For example, MOM provides the following:

- **Managing**—MOM brings 24x7 monitoring to all aspects of your Windows server-based environment. It provides proactive alerting and responses by using built-in expertise to recognize conditions that will lead to failure in the future. MOM can execute tasks manually and even automatically in response to events or conditions to resolve problems.
- **Tuning**—To assist in tuning, MOM collects long-term trending data, provides suggestions for improving performance, and allows you to compare the results of performance adjustments to historical performance. Comparing results addresses a fundamental problem with performance tuning, which is making sure that the tuning actually improves performance! MOM provides the empirical data needed to ensure that tuning works.
- **Auditing**—Windows 2000 and 2003 provide excellent auditing capabilities. The problem is that system and security administrators rarely review the Security Event logs for any potential breaches or suspicious

activity. The sheer volume of data and number of servers usually precludes even just glancing at the data, much less mining those logs for subtle security problems. MOM tirelessly monitors the logs on every server around the clock, even correlating individually innocent events to identify potential hacking attempts or security breaches.

This chapter introduces Microsoft Operations Manager 2005. MOM is Microsoft's software solution for facilitating server operations management, now in its second major release. MOM 2005 is Microsoft's latest version of the product and contains many improvements over the previous version, including better scalability, enhanced security, and features such as tasks and diagrams. The chapter also discusses the concepts behind operations management and examines Microsoft's management approach and Dynamic Systems Initiative (DSI). We provide an overview and comparison of two methodologies for approaching operations management: the Information Technology Infrastructure Library (ITIL) standard and the Microsoft Operations Framework (MOF). Additionally, we discuss the operations management basics of event and performance management.

In a Nutshell: Ten Reasons to Use MOM

So, why use MOM? You may be thinking that the features sound "cool" but also are wondering why you need it. Management seldom approves new systems just because they are "cool." Although this book will go over all the features and benefits of MOM 2005, it helps to have a few short answers here that bring it home.

Here are ten compelling reasons for using MOM:

1. You do not have time to check the event logs on mission-critical servers at least daily.
2. You do not know what your servers are doing at any given time. This includes things such as how many users are accessing a web server, how utilized the servers are, or how much free disk space you have left.
3. It feels like the Information Technology (IT) version of the movie *Groundhog Day* where you must solve the same problems over and over again every day in exactly the same way—except that unlike the movie, here you can really die.
4. You do not have enough internal expertise to solve the problems that come up, as they come up.
5. Users alert you to problems in the systems when they start calling you. Although this system is effective in getting your attention, it usually means that you are in hot water already—and phone calls are annoying.
6. You run out of resources such as disk space and wish you knew in advance to perform upgrades or load balance files across your servers.

7. When a virus outbreak hits, it takes you hours to figure out what service packs and hotfixes were applied to each server, and then it's usually not good news and you probably haven't tested them yet.
8. When management asks you for a report on the systems, which usually is to justify *your* purchase requests, it takes days or weeks to get the information in a form they will accept.
9. You have better things to do than watch servers all day. And night. Or during vacation.
10. Your job and compensation depend on server and application reliability and performance—and you find that out the hard way during your performance review.

If any of these points resonate with you, you owe it to yourself to investigate MOM. These pain points are common to almost all users of Microsoft technologies, and MOM eliminates all of them to a great degree.

However, the biggest reason of all for using MOM is *peace of mind*. Deploying MOM allows you to relax, secure in the knowledge that MOM is watching your back. After all, what's a mother for?

The Problem with Today's Systems

From the perspective of operations management, today's information technology has a number of problems. These include information isolation, no built-in notification systems, no historical information, and concentrated expertise. Some problems are nonintuitive, such as missed events where something does *not* happen when it should. MOM addresses many problems, including

- Islands of information
- No notification of events
- No historical information
- Lack of expertise
- Missed events
- False alarms

These problems manifest themselves in all IT shops with varying degrees of severity. Let's look at what these are in detail.

Why Do Systems Go Down?

It is helpful to examine why systems go down. The following is a rough grouping of reasons for systems going down. Figure 1.1 illustrates the breakdown of reasons for system

outages, based on our personal experiences and observations, and the following list describes some of the reasons.

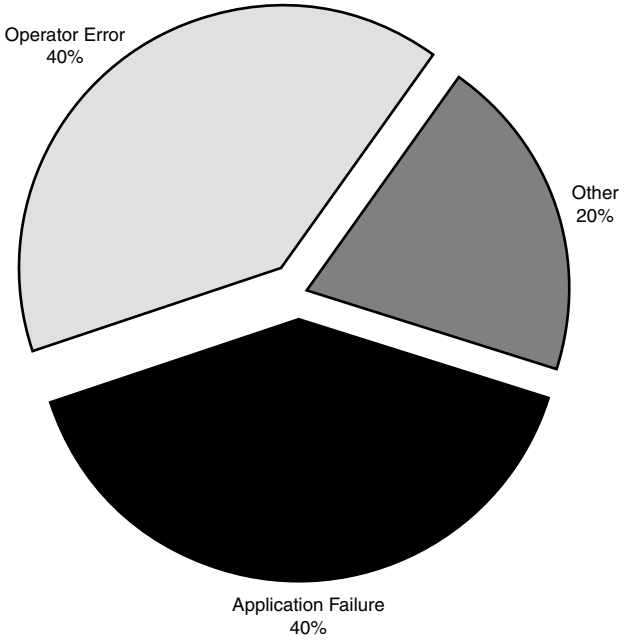


FIGURE 1.1 Causes of system outages.

- **Software errors**—We have found that software is responsible for somewhat less than half the errors. These errors include software coding errors, software integration errors, data corruption, and such.
- **User errors**—Operators cause a little less than half the errors. Here we include systems incorrectly configured, failure to catch warning messages that turn into errors, accidents, and so on.
- **Miscellaneous errors**—This last category is relatively small. Causes of errors here include disk crashes, power outages, viruses, disasters, and so on.

As you can see, software level errors and user errors together account for the vast majority of failures. The surprise is that hardware failures account for a only small percentage of problems, which is a tribute to modern systems such as Redundant Array of Independent Disks (RAID) and other mechanisms deployed to provide server and application redundancy.

This means that to reduce system downtime, you really need to attack the software error and user error components of the equation. That is where you will get the most ”bang for the buck.”

Islands of Information

Microsoft Windows 2003 and applications that run on it such as Microsoft Exchange and Microsoft SQL Server expose an incredible amount of information in event logs, performance counters, and other logs. However, the data is isolated and server-centric. As you can see in Figure 1.2, we essentially have islands of information.

FIGURE 1.2 Islands of information.

We can find some isolated information in these locations:

- **Event logs**—Events are generated by the Windows operating system and by applications. These include errors, warnings, and information and auditing events. These events are stored locally on each server.
- **Performance counters**—Windows and applications expose detailed performance information through performance counters. This includes processor utilization, memory utilization, network statistics, disk free space, and thousands of other pieces of operational information.
- **Windows management instrumentation (WMI)**—WMI provides access to an incredible amount of information, from high-level status of services down to hardware information.
- **Expertise**—Consultants, engineers, and subject matter experts all have information locked up in their heads. This is as much an island of information as any of the numeric values in the logs or counters.

All this information is captured through event logs, performance counters, file-based logs, and experiences but is lost over time. Most logs roll over, are erased to clear space, or are eventually overwritten. Even if the information is not lost over time, it is usually not reviewed regularly as a maintenance practice.

Additionally, most application information in Windows 2000 and Windows Server 2003 is server-centric and is usually stored on the server and specific to the server where the application resides. There is no built-in, system wide, cross-server view of critical information.

These islands of operations information, where operations personnel are stranded on any given island, make it difficult to get to needed information in a timely or effective manner.

No Notification

No one may know when important events occur in a typical nonmanaged IT environment. The task of going to each server and reviewing the event logs on a timely basis is a huge undertaking for most administrators. The event logs capture information, but they roll over and are overwritten without ever being looked at. The information is lost.

There is an old philosophical question: If a tree falls in a forest and no one hears it, does it make a sound?

The operations management equivalent is: If an event is logged on a system and no one knows about it, does logging it make a difference?

The answer to the latter is definitely "no"; the event may as well have not been logged. This loss of information can affect the long-term health of the system. This matters because if its occurrence were known you would be able to prevent potential outages.

For example, in one situation, an Exchange server at a large real estate firm was getting 1018 errors logged in the Application event log for several months, but the administrators never looked in the logs to catch it. A 1018 error indicates an Exchange database error and is a severe error requiring immediate action. When the server ultimately crashed, the backups were no good—they had been overwritten with corrupt databases. This led to an expensive disaster recovery using the services of a consulting firm, with loss of critical messaging data and job loss to the staff held responsible.

Ultimately, information is only informative if you are made aware of it, and it is only as good as what you do with it. To put this another way, most IT shops have many trees falling with no one hearing about it until it is too late.

No Historical Information

Sometimes information about events is captured, but you cannot look back in time and see whether this is an isolated instance or part of a pattern. Without the historical context, it is difficult to understand the significance of any given event. This is particularly true of performance data.

Let's say a technical consultant is brought in to review a system's performance problems. To prove there is a problem, the IT staff points out that users are complaining about performance and that the disk or CPU is only 50% utilized. In and of itself, this does not tell us anything. It could be that the disk or CPU is normally 65% utilized and the

problem is really a network utilization problem, which suggests reducing the load on the server as a remedy.

As a technical expert, the consultant would take care to develop a hypothesis and test it, which can take time and cost money. In contrast, many IT shops just buy more hardware only to find that this does not improve performance. If they had historical records, they would have seen that utilization actually dropped at the same time that users started complaining and would have been able to look elsewhere to find the network problems. Ideally, you want to be able to look back at historical information to troubleshoot and detect trends.

No Expertise

Are you missing the in-house expertise to diagnose some of the messages or trends that appear on your Windows servers and server-based applications? Does it cost you an arm and a leg to call in consulting resources, only to find that the events were actually not all that severe?

The bottom line is that the expertise may not be available when you need it, leading to either missed diagnostic opportunities or higher operational costs. Missed diagnostics opportunities translate to system outages and ultimately higher operational costs as well, when emergency measures may need to be taken to resolve problems.

Missed Events

Sometimes problems can be detected by what did not occur, rather than by what did occur. A good example of this can be found in the case of backups. Whether the backup is successful or fails, you get an event and some type of notification.

However, what happens if the backup doesn't fail or succeed, but just doesn't happen? If you are not looking closely, you will likely miss that until later. We know a case of a large educational institution that was performing backups but missed one server during the initial configuration. After a server crash, they went back to restore and only then noticed that the server was not being backed up. Even though they had configured all of the backup jobs to generate success notices and were notified of failures, the missing server never generated a successful or failure notification and so was missed—with serious consequences to management, faculty, staff, and students.

Sometimes when you do not receive a notification or event it is a cue to take action. The bottom line here: You need to be able to test for the absence of an event.

False Alarms

Even when you are notified of an event, sometimes it is difficult to tell whether you really have a problem. Windows 2000 and 2003 and the applications that run under them are good about generating errors, warnings, and informational events. The problem is that it can be difficult to tell which of these are normal operating events and which are errors needing corrective action.

False alarms are usually the result of lack of knowledge or lack of filtering. Sometimes an event looks ominous to the untrained eye, such as a warning event 11 from w32time in the System Event Log, indicating that a Network Time Protocol (NTP) server could not be reached. In reality, this is a normal event and is not a problem. However, several of these errors in a row might indicate a problem needing action.

What Is Operations Management?

Operations management is a process aimed at improving the reliability and availability of computer applications and services by addressing the problems discussed in the previous section. Operations management bliss is not attained merely by running setup.exe to install a "management" application; the process of operations management is a combination of people, procedures, and tools—all three are necessary, and the absence of one component can put an entire enterprise solution at risk. At a more granular level, operations management is about correlating what may appear to be seemingly unrelated events and data across machines to determine what information is significant to your operational environment versus what is not.

Operations management is also about managing the ongoing activities that Information Technology personnel perform on various IT components with the goal of improving the performance of one's business organization. How does operations management accomplish this? As IT operations grow in size and impact, it quickly becomes apparent that effectively managing complex production environments requires defining and utilizing standardized methodologies and approaches for managing servers. Once a business relies on IT to maintain daily operations, a disciplined and informative methodology is necessary to help ensure IT is supporting the organization's business goals and objectives. These goals typically include reducing costs, increasing productivity, and providing information security.

Reducing costs and increasing productivity is important because, in addition to taking up a significant part of the IT budget, the business impact of failed systems or performance degradation can be devastating to the entire enterprise—resulting in increased operational costs, decreased quality of service, and lost revenue and profit. Time, after all, is money! Information security is also imperative as the price tag of compromised systems and data recovery from security exposures can be large, and those costs continue to rise each year.

The Cost of Downtime

As an example, let's consider a simplified example of the impact of temporarily disrupting an e-commerce site normally available 7x24. The site generates an average of $4,000 per hour in revenue from customer orders for an annual value in sales revenue of $35,040,000. If the website were unavailable for six hours due to a security vulnerability, the directly attributable losses for the outage would be $24,000.

This number is only an average cost; most e-commerce sites generate revenue at a wide range of rates based on time of day, day of week, time of year, marketing campaigns, and so on. Many times, the outage will occur during peak times when the system is already stressed, greatly increasing the cost of a 6-hour loss.

The outage may also cause some customers to find alternative vendors, resulting in some permanent loss of users and making the revenue loss even higher than the direct loss of sales.

There are also possible indirect costs of the outage. The company may decide to spend additional money on advertising to counter the ill will created when customers could not reach the site. The costs from the 6-hour outage can be far higher than its simple hourly proportion of time applied to an average revenue stream.

As part of an operations management plan, any company with more than nontrivial IT requirements can benefit from software tools to automate tasks such as managing server networks, tracking desktop systems, and enforcing security policies. Microsoft software addresses this area through two key products—Systems Management Server (SMS) and MOM.

SMS is Microsoft's product for change and configuration management on the Microsoft Windows platform, reducing the operational costs of managing and deploying software—enabling organizations to distribute relevant software and updates to users quickly and cost effectively. MOM provides you with knowledge to reduce the complexity of managing your IT infrastructure environment and lower your cost of operations. Keep in mind however, that SMS and MOM are merely tools; they enable you to meet objectives using software for automating the process.

Microsoft's Management Approach

Microsoft utilizes a multi-pronged approach to management. This strategy includes

- Making Windows easier to manage by providing core management infrastructure and capabilities in the Windows platform itself, allowing business and management application developers to improve their infrastructures and capabilities. Microsoft has decided that improving the manageability of solutions built on Windows Server System should be a key driver shaping the future of Windows management.
- Building complete management solutions on this infrastructure, either through making them available in the operating system or by using management products such as SMS, MOM, Application Center, and the System Center family.

  Application Center 2000 is a deployment and management tool for high-availability web farms. More information is available at www.microsoft.com/applicationcenter.
- Integrating infrastructure and management by exposing services and interfaces that can be utilized by applications.
- Moving towards a standard Web Services specification for system management. WS-Management is intended to provide a universal language that all types of devices can use to share data about themselves, enabling them to be more easily managed.
- Taking model-based management (used with the Dynamic Systems Initiative, discussed in the next section of this chapter) to implement synthetic transaction

technology. Future versions of Operations Manager are intended to deliver a service-based monitoring set of scenarios, enabling you to define models of services to deliver to end users.

Microsoft's Dynamic Systems Initiative (DSI)

A large percentage of IT departments' budgets and resources typically focus on mundane maintenance tasks such as applying software patches or monitoring the health of a network, without leaving time or energy to focus on more exhilarating (and more productive) strategic initiatives.

The Dynamic Systems Initiative, or DSI, is a Microsoft and industry strategy intended to enhance the Windows platform, delivering a coordinated set of solutions to simplify and automate how businesses design, deploy, and operate their distributed systems.

DSI focuses on automating data-center operational jobs and reducing associated labor through self-managing systems. Can management software be made clever enough to know when a particular system or application has a problem and then dynamically take actions to avoid that? Consider the scenario where, without operator intervention, a management system starts an additional web server because the existing web farm is overloaded from traffic. Rather than being far-fetched, this particular capability is already available today with Microsoft Application Center 2000; DSI aims to extend this type of self-healing and self-management to other operations.

In support of DSI, Microsoft has invested heavily in three major areas:

- **Systems designed for operations**—Microsoft is delivering development and authoring tools—such as Visual Studio—that enable businesses to capture and edit system knowledge and facilitate collaboration among business users, project managers, architects, developers, testers, and operations staff. Additionally, Microsoft servers and many third-party applications will be enabled to capture information necessary to dramatically improve deployment and management.
- **An operationally aware platform**—The core Windows operating system and its related technologies are critical in helping solve everyday operational challenges. To accomplish this, services within the operating system must be designed for manageability. Additionally, the operating system and server products must provide rich instrumentation and hardware resource virtualization support.
- **Intelligent management tools**—The third and most critical piece in DSI contains the management tools for leveraging the operational knowledge captured in the system, providing end-to-end automation of system deployment.

Microsoft's Solutions for Systems Management

End-to-end automation could include updating, monitoring and change/configuration, and rich reporting services. Microsoft's current offerings for these capabilities include SMS 2003 and MOM 2005. System Center Reporting Manager 2006 incorporates

"better together" reports by consolidating event and performance information from MOM 2005 and change and configuration management data from SMS.

The short-term product components of DSI are Microsoft Windows Server Update Services (WSUS), a series of MOM management packs for Windows Server System applications, Visual Studio 2005, and Microsoft's other management-related offerings—SMS, Windows Server Automated Deployment Services (ADS), Application Center, and System Center components including Data Protection Manager, Reporting Manager, and Capacity Planner. The philosophy behind DSI is that Microsoft products should be patched in a simplified and uniform way, that all Microsoft server applications should be optimized for management to take advantage of MOM 2005, and that developers should have tools (in Visual Studio) to design applications in a way that makes them easier for administrators to manage after those applications are in production.

With DSI, Microsoft utilizes a nontraditional approach to systems management. DSI employs an application development standpoint rather than a more customary operations perspective that concentrates on automating task-based processes. DSI is about building software that enables knowledge of an IT system to be created, modified, transferred, and used throughout the life cycle of that system. DSI's core principles—knowledge, models, and the life cycle—are key in addressing the challenges of complexity and manageability faced by IT organizations.

Central to DSI is an Extensible Markup Language (XML)-based schema called Systems Definition Model (SDM). The SDM can be utilized in architecting software and hardware components. The model is used to create definitions of distributed systems. Businesses can use SDM to take an entire system and generate a blueprint of that system. The blueprint defines system elements and captures data pertinent to development, deployment, and operations—making that model relevant across the entire IT life cycle. SDM is a core technology around which we should see many future DSI components and products being developed.

IT Infrastructure Library (ITIL) and Microsoft Operations Framework (MOF)

ITIL is widely accepted as an international standard of best practices for operations management and has been used by Microsoft as the basis for the MOF, its own operations framework.

What Is ITIL?

As part of Microsoft's management approach, the company relied on an international standards-setting body as its basis in developing an operational framework. The British Office of Government Commerce, or OGC, has developed best practices advice and guidance on the use of information technology in service management in operations. The OGC publishes the IT Infrastructure Library, known as ITIL.

ITIL provides a cohesive set of best practices for IT Service Management (ITSM), maintained by the OGC and supported by publications, qualifications, and an international users group. These best practices consist of a series of books giving direction and guidance on provisioning quality IT services and facilities needed to support Information Technology.

Started in the 1980s, ITIL is under constant development by a consortium of industry IT leaders. The ITIL covers a number of areas and has its primary focus on ITSM; its IT Infrastructure Library is considered to be the most consistent and comprehensive documentation of best practices for IT Service Management worldwide.

ITSM can be considered a top-down, business-driven approach to the management of IT, specifically addressing the strategic business value generated by the IT organization and the need to deliver high-quality IT services to the business organization. ITSM itself is divided into two main areas: Service Support and Service Delivery. ITSM is designed to focus on the people, processes, and technology issues faced by IT, analogous to the focus in operations management.

ITIL describes at a high level "what you must do" and why but does not describe how you are to do it. A driving force behind its development was the recognition that organizations are increasingly dependent on IT for satisfying their corporate aims and meeting their business needs, leading to an increased requirement for high-quality IT services.

ITIL also specifies keeping measurements, or metrics. Measurements can include statistics such as the number and severity of service outages, along with the amount of time it takes to restore service. You can use metrics to quantify to management how you are doing, and this information can be particularly useful for justifying resources during the next budget process!

What Is MOF?

ITIL is generally accepted as "best practices" for the industry. Being technology-agnostic, it serves as a foundation that can be adopted and adapted to meet the specific needs of various IT organizations. Microsoft chose ITIL as the foundation for its operations framework, such that the Microsoft Operations Framework (MOF) gives prescriptive guidance in operating Microsoft technologies in conformance with the descriptive guidance in ITIL. MOF is a set of publications providing both descriptive (what to do and why) and prescriptive (how to do) guidance on IT service management.

The key focus in the MOF development was providing a framework specifically geared toward managing Microsoft technologies. Microsoft created the first version of the MOF in 1999. MOF is designed to complement Microsoft's previously existing Microsoft Solutions Framework (MSF) used for solution and application development. Together, the combined frameworks provide guidance throughout the IT life cycle, as shown in Figure 1.3.

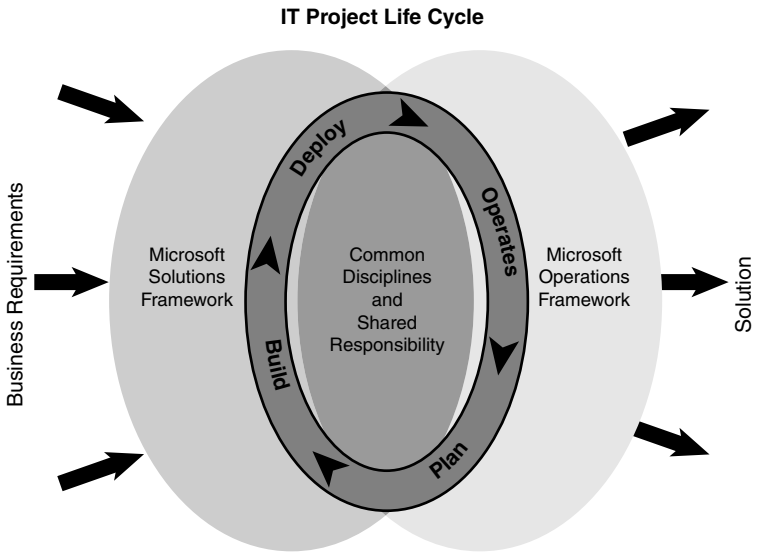


FIGURE 1.3 The IT life cycle and Microsoft frameworks.

At its core, the MOF is a collection of best practices, principles, and models. The MOF provides direction for achieving reliability, availability, supportability, and manageability of mission-critical production systems, focusing on solutions and services using Microsoft products and technologies. MOF extends ITIL by including guidance and best practices derived from the experience of Microsoft's internal operations groups, partners, and customers worldwide. MOF aligns with and builds on the IT service management practices that have been documented within ITIL—enhancing supportability built on Microsoft's products and technologies.

MOF uses a process model that describes Microsoft's approach to IT operations and the service management life cycle. The model organizes the core ITIL processes of service support and service delivery, and adds additional MOF processes into the four quadrants of the MOF process model, as illustrated in Figure 1.4.

It is important to note that the activities pictured in the quadrants illustrated in Figure 1.4 are not necessarily sequential and can occur simultaneously within an IT organization. Each quadrant has a specific focus and tasks, and within each quadrant are policies, procedures, standards, and best practices that support specific operations management–focused tasks.

MOM's management packs can be configured to support operations management tasks in different quadrants of the MOF Process Model. Let's look briefly at each of these quadrants and see how Microsoft Operations Manager can be used to support MOF:

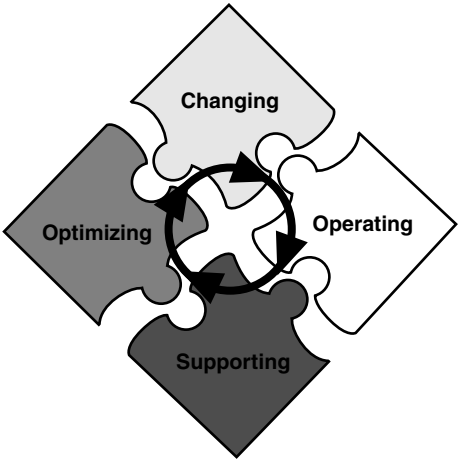


FIGURE 1.4 The MOF process model.

- The Changing quadrant represents instances where new service solutions, technologies, systems, applications, hardware, and processes are introduced.

  As you add new components to your environment, you should investigate whether a Microsoft or third-party management pack is available to monitor that particular application, system, or hardware solution. (If a management pack is not available you can define your own, describing the "vital signs" and monitoring attributes of that application.)

- The Operating quadrant concentrates on performing day-to-day tasks efficiently and effectively.

  MOM includes operational tasks that you can initiate from the Operations console. These tasks are made available with various management packs, and you may add your own as well.

- The Supporting quadrant represents the resolution of incidents, problems, and inquiries, preferably in a timely manner.

  MOM is all about monitoring daily operations. Management packs provide the capability, for knowledgeable users, to interpret and act on information gathered from each monitored system so as to resolve any difficulties.

- The Optimizing quadrant focuses on minimizing costs while optimizing performance, capacity, and availability in the delivery of IT services.

Service Level Agreements (SLAs) and Operating Level Agreements (OLAs) are tools many organizations use in defining accepted levels of operation and ability. MOM specifies SLAs with Alert Resolution States. Additional information regarding the MOF Process Model can be found at http://go.microsoft.com/fwlink/?LinkId=50015.

MOF Does Not Replace ITIL

Microsoft believes that ITIL is the leading body of knowledge of best practice; for that reason it uses ITIL as the foundation for its MOF framework. Rather than replacing ITIL, MOF complements it and is similar to ITIL in several ways:

- MOF (with MSF) spans the entire IT life cycle.
- MOF and ITIL are both based on best practices for IT management, drawing on the expertise of practitioners worldwide.
- The MOF body of knowledge is applicable across the business community—from small businesses to large enterprises. MOF also is not limited to those using the Microsoft platform in a homogenous environment.
- As is the case with ITIL, MOF has expanded to be more than just a documentation set. For example, MOF is a core component of the *MOM 2005 Solution Accelerators*, which are predefined solutions giving technical and prescriptive guidance for MOM 2005 capabilities in specific aspects of operations management.

The MOM Solution Accelerators

As discussed in Chapter 19, "Interoperability," the MOM 2005 Solution Accelerators focus on streamlining alert management and improving service continuity. Information on the Solution Accelerators is available at http://go.microsoft.com/fwlink/?LinkId=46590.

Additionally, Microsoft and its partners provide a variety of resources to support MOF principles and guidance, including self-assessments, IT management tools that incorporate MOF terminology and features, training programs and certification, and consulting services.

Managing Events and Performance

Although ITIL and MOF are utilized to define management approaches, strategies, and solutions, day-to-day operations in today's world are at a different level of granularity. Typically, today's computing environments consist of distributed systems where work is performed utilizing dispersed servers—because distributed computing often requires using numerous machines that may be in multiple locations. While an overall management strategy is necessary for preventing chaos in operations and systems management, daily management of production server environments also requires being thoroughly aware of the operational health and security of those systems—are they performing the tasks they are meant to, are they the focus of a hacker, or are they even reachable across the network?

Operations management is concerned with monitoring your servers to ensure that they maintain a required level of performance. Looking specifically at the Windows platform, Microsoft provides a number of basic monitoring utilities with the Windows Server

product. These tools incorporate core event monitoring, performance monitoring, and management components such as the Event Viewer and Performance Monitor.

However, understanding the significance of the information made available with such utilities can be a daunting task, particularly when the quantity of servers is large and the complexity of the environment seems overwhelming. Although these basic tools are included with Windows Server, they provide a view of the trees without being able to see the forest—they give a detailed view of a single server and were not designed for scalability or for easy diagnosis of information to resolve problems occurring across multiple systems.

Because these utilities only provide raw data, using such data effectively requires personnel with the knowledge to select, understand, filter, and interpret that data. These tools typically only show pieces and parts of the overall picture, and additional data may be required from different sources.

The information spewing from these systems consists of thousands of events and other types of operational data that can be captured from a single server and brings to mind the term "drinking water from a fire hose" as shown in Figure 1.5—that is, being overwhelmed with a gushing stream of facts and figures coming at you with tremendous built-up pressure. Making sense of all that data, or "taming the fire hose," is a challenge facing IT shops of all sizes, and one that MOM is designed to address.

FIGURE 1.5 Drinking water from a fire hose.

Unlike scenes in the movie *The Matrix*, numbers are not just pouring vertically down the screen, but neither do you need the ability to jump from roof to roof or dodge bullets to be able to decipher them. You merely need the tools and products available to mere mortals.

The Solution: MOM 2005

MOM 2005 solves these operation management problems and is a key component in Microsoft's management strategy. MOM is a comprehensive operations management solution that uses an agent-based centralized management model to localize data collection, yet centralizes the collected data and configuration of its agents. MOM 2005 provides the following benefits:

- Event-based monitoring
- Easily deployed and scalable infrastructure
- Effective system availability and performance tracking

An agent operates under a sophisticated set of rules, collected in management packs. These management packs allow the rules to be applied as a group to just the systems that need them. Problems identified by these rules can be acted on by operational and systems personnel, and the results collected by this process can be analyzed and published using MOM's reporting capabilities.

To put MOM's capabilities in a clearer context, we will discuss the key technical features as they relate to the issues identified earlier in "The Problem with Today's Systems" section of this chapter.

Connecting Information

MOM solves the islands of information problem by collecting information from the different islands. It monitors event logs, performance monitor counters, application programming interfaces, and WMI information, locally gathering the data from each monitored server, centrally storing it, and taking action as appropriate. MOM also provides a centralized console from which you can monitor the operational status of the entire network. Figure 1.6 shows the state view of the monitored organization. The view shows that there is currently a problem area, within the SQL subsystem on the computer Fountain. You also see in Figure 1.6 that the Aurora Exchange computer is highlighted, and that there are 4 open alerts, 7,922 events, and the last heartbeat was on 7/5/2006 at 10:09 AM. Even though the state shows all as green (healthy), several yellow triangles in the leftmost (State) column indicate that there are outstanding Error and Warning alerts for those computers. These might indicate problems for investigation or problems that have resolved themselves.

MOM uses distributed event management, meaning that events collection and handling of information is distributed across various computers, as opposed to centralized event management. Distributed event management has the following advantages over centralized event management:

- Local information collection
- Better fault tolerance
- Reduced network footprint
- Better response times

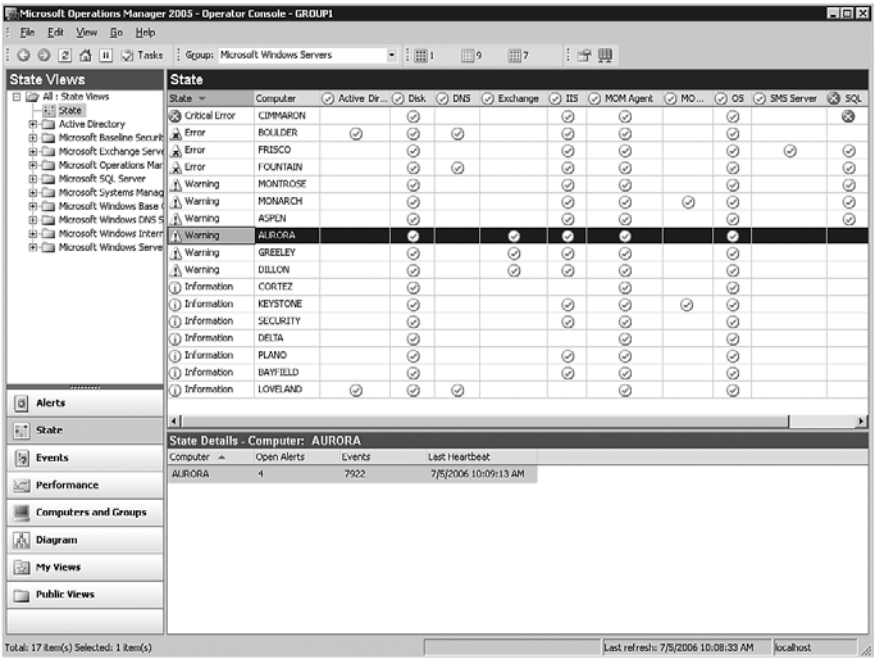


FIGURE 1.6 Microsoft Operations Manager operators console.

The advantages of a distributed model are that information is collected, buffered, and processed locally. This model allows the management infrastructure to be fault-tolerant and flexible to conditions such as network outages, without losing valuable information. When a network outage is in effect, the local agents keep collecting information and responding to alert conditions. A distributed model also reduces the impact of the data collection on the network by forwarding only data that needs to be forwarded. The agent on the local system compresses the data stream to reduce the footprint even further. A distributed model also allows the infrastructure closest to the source to respond to alert conditions. This can dramatically reduce the response time in a large enterprise, where events might need to bubble up through various management levels to finally reach a central console.

The key to this process of connecting information is the intelligent agent. MOM installs an agent on all monitored servers, in effect distributing the operations management intelligence. (MOM 2005 also allows agentless monitoring of a limited number of servers.) This allows the monitored systems to forward only the information deemed important, rather than everything. It also allows the monitored system to continue to collect operations data even if communications with the central console is disrupted. This data will be forwarded once communications are reestablished.

Information is collected locally using an agent service, although the centralized server ultimately receives the information. It gathers the information from all the islands and stores it in a common database. This database is centrally located and stored on an SQL

Server system, allowing MOM to correlate and respond to networkwide events, such as a virus outbreak or an attempt to breach security on several systems at once. MOM monitors all the time, making sure that no events are missed.

The agents process rules, which specify what data to collect and what to do about it. Rules can filter information and aggregate and consolidate the collected information. These rules are really the core functionality of the MOM infrastructure and are covered in detail in Chapter 14, "Monitoring with MOM." Rules are logically collected into rule groups or management packs, which are applied as a unit. Using management packs is discussed in Chapters 15 through 18.

The centralized storage of information also eliminates our islands of information issue by allowing consolidated views and reports of the many different islands of information across many different servers. For example, an administrator can produce a report that compares the error events, CPU performance, message queues length, and network interface performance on Exchange servers in different parts of the network at the same time. Without MOM 2005, providing this information would require multiple interfaces and tools.

Although following a distributed event model, MOM centralizes the storage of its information. This allows the system to respond to complex conditions where several events taken independently would not constitute a problem, but taken together demand immediate action.

For example, if the Contoso Company has a network load-balanced farm using four web servers to provide web services, the failure of any one system would not jeopardize the overall service. Arguably, that is the purpose for having load-balanced servers. However, the failure of two or three of these servers would constitute a critical condition requiring immediate attention. MOM is capable of generating merely an error alert if any individual server fails, but generates a critical error alert if two or more servers fail.

Operations Notification: Errors and Availability

MOM 2005 solves the notification problem by automatically detecting and responding to events of all types. While collecting the information, responses to conditions can be triggered at each collection point in the architecture. Figure 1.7 shows the types of events that MOM is collecting. The highlighted information event indicates that the defragmentation of the Exchange database completed successfully for Public Store on the Aurora Exchange server. There are warning events that indicate that there are mailboxes for users with disabled accounts.

Interestingly, some of the events are in fact generated by synthetic transactions. These are activities initiated by MOM itself to test the monitored systems. For example, in Figure 1.7 the information event at 1:15:02 AM is a result of a successful login by the MOM agent on the Aurora computer to test availability via the Messaging Application Programming Interface (MAPI). MOM initiates a number of different transactions of this type to verify that systems are operational and that their performance is up to par.

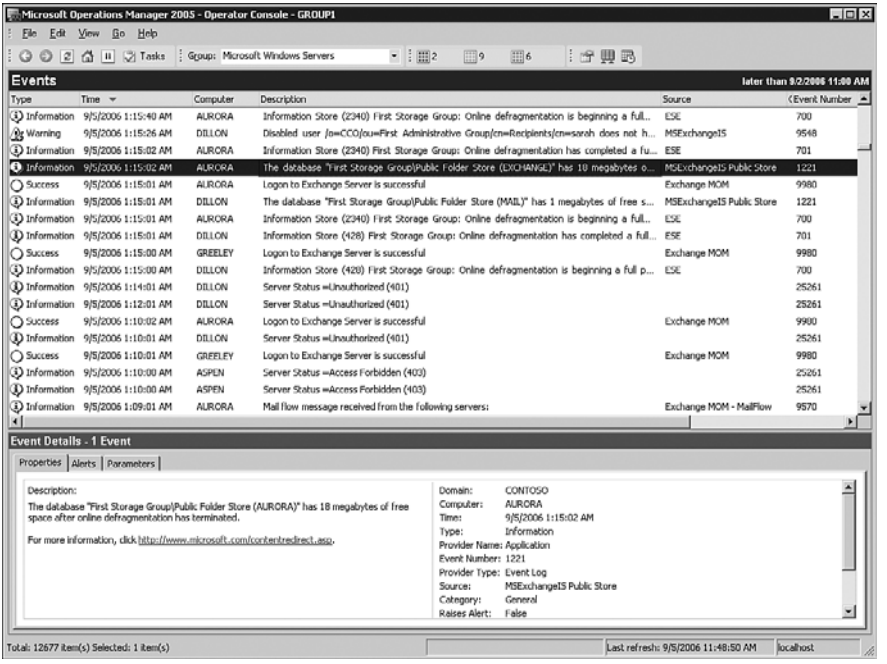


FIGURE 1.7 Event collection.

At the bottom left-hand corner of Figure 1.7, you can see that MOM has collected more than 12,000 events in the previous three days. The selection criteria are indicated in the upper right-hand corner of the figure, which are all events since 9/2/06 11:00 AM. Although MOM has collected all these events, it has in fact looked at and not collected even more. These events are processed by the local agent and analyzed based on the business logic in MOM's rules, and a decision is made whether to send the event to the central server, known as a management server.

The process is carefully designed to approach the best of all possible worlds. The work of collecting and initially processing the information is done by intelligent agents on the monitored servers. This reduces the load that MOM places on the management server because information is centrally acted on only as necessary. It also allows the local agents to continue to respond to alert conditions even if there is a disruption in communication to the management server. This preprocessing helps keep the traffic flow from the agents lean and the database storage footprint light. Even so, an administrator would not want to be notified for all the myriad events collected by MOM 2005. Accordingly, MOM is selective about what alerts are raised.

Alerts can be generated by any rule in response to a single event or multiple events. These events can even come from multiple sources (that is, different islands of information). Although more than 15,000 events are collected by MOM, Figure 1.8 shows only three alerts generated. The highlighted event in Figure 1.8 shows an alert generated by high memory utilization on the Cortez server. Although we see three separate alerts in the

console, some may have multiple events behind them. For example, the critical error alert modified at 3:30:01 AM was the third event that triggered the alert. Rather than generating an alert for each event, MOM consolidates the events into a single alert with a repeat count. You will notice that the repeat count starts at 0, so the repeat count of 2 indicates that there were two other events in addition to the current one for a total of three events.

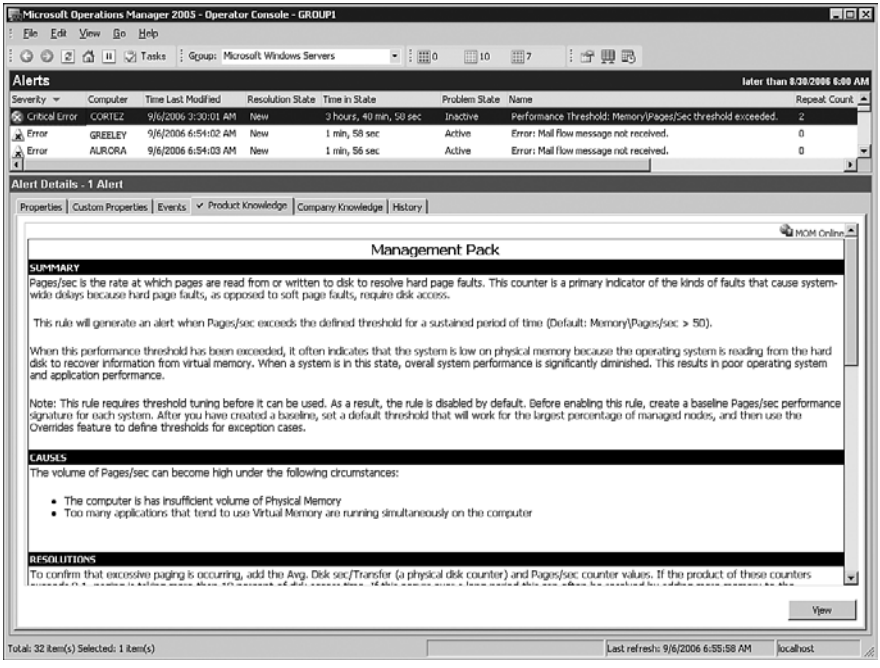


FIGURE 1.8 Alerts collected in the Operator console.

In addition to generating alerts, MOM can also send out notifications based on the severity of the alert. Alerts can notify administrators in a variety of ways, such as by sending a network message, sending an email message, generating a Simple Network Management Protocol (SNMP) trap to integrate with another management system, or launching a script for complex processing. This ensures that even if an alert is generated, it does not intrusively notify you unless it truly needs to.

Security Policy Notification: Enforcement and Auditing

A big problem in IT today is the distributed nature of security within Microsoft applications. Many administrators have local administrative access to servers, allowing them to modify things such as system and security logs. This access can be used to circumvent security policies, ostensibly with the purpose of getting the job done. This is a gaping hole in any organization trying to maintain tight security. You need notification when there are security changes.

MOM 2005 can monitor for any changes in configuration and alert the appropriate security personnel of violations of security policy. In addition, the local agent immediately forwards event log entries to the central console, in effect moving them outside the control of the local administrator. Even if the local administrator attempts to cover her tracks by clearing the event logs, MOM will have sequestered the information in its central repository. If the local administrator attempts to circumvent the process by shutting down the agent, the central console detects that and can generate an appropriate alert to the security officer.

With security and configuration information safely and securely stored centrally, the security officer can generate reports and analyze the data to look for potential security problems. MOM can even be configured to automatically detect and alert to those security problems.

Historical Information

MOM allows the information it gathers to be viewed quickly and effectively. It is all well and fine that information is collected, but it is for naught if that information is not easily accessible. MOM 2005 presents that information in several ways to make it easy to view, print, or publish.

The data collected by the rules includes event and performance statistics, invaluable information for analyzing what your servers and services are doing over the long term. To help review and understand the long-term trends and conditions of the servers and applications, MOM generates reports both automatically and ad hoc. For example, in Figure 1.9 you can see a CPU utilization spike of 80% on 9/5/2006 at about 1 AM for about 20 minutes on the computer Loveland. This view gives quick access to information as it is collected and the capability to adjust the view of that information quickly, for example to compare it with another system or graph different times.

However, this particular view does not tell us if this is normal performance for the computer. To put the CPU utilization spike in context, we would want to know what the long-term CPU utilization looks like for that system. We can access the long-term view of historical data using the MOM Reporting component, which is based on Microsoft SQL Server Reporting Services (SRSS). As shown in Figure 1.10, the processor utilization for the week prior shows a regular daily spike—so the utilization spike detected in Figure 1.9 is probably normal. Sometimes knowing what is normal is half the battle!

MOM Reporting allows you to generate sophisticated reports complete with titles, numeric information, text information, graphs, and charts. Views allow you to see a quick view of data, which can also be displayed as text or graphs. Reports are static once generated, whereas views are active and update as the data changes. Reports can be saved in PDF format or published as HTML files. The HTML option is particularly powerful because it allows reports to be generated and published for general viewing on an intranet site. The only requirement is having a browser and access to the site, which allows IT to publish routine stats, uptime, and so on, easily and effectively. We discuss reporting capabilities in greater detail in Chapter 21, “Using and Developing Reports.”

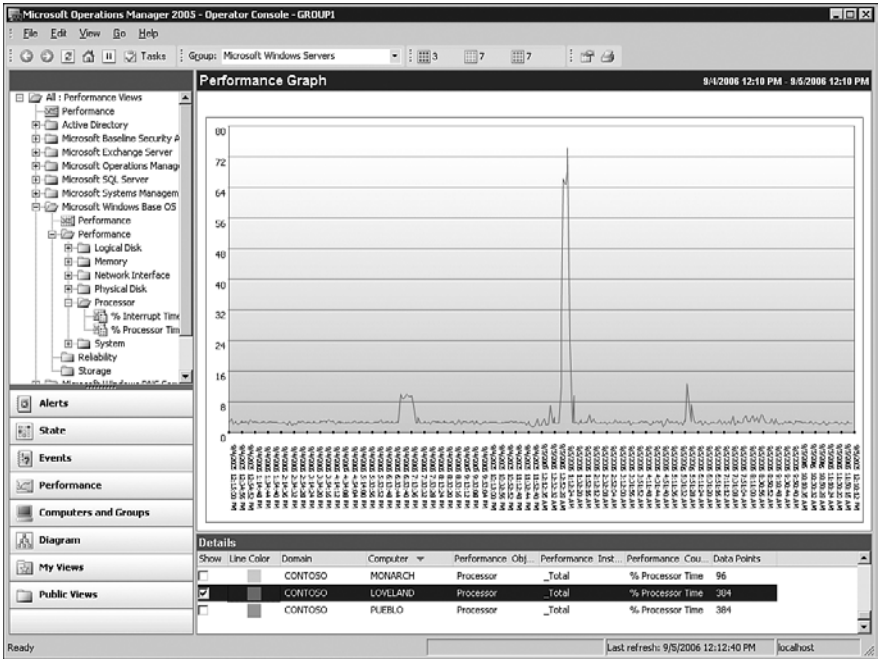


FIGURE 1.9 CPU performance analysis view.

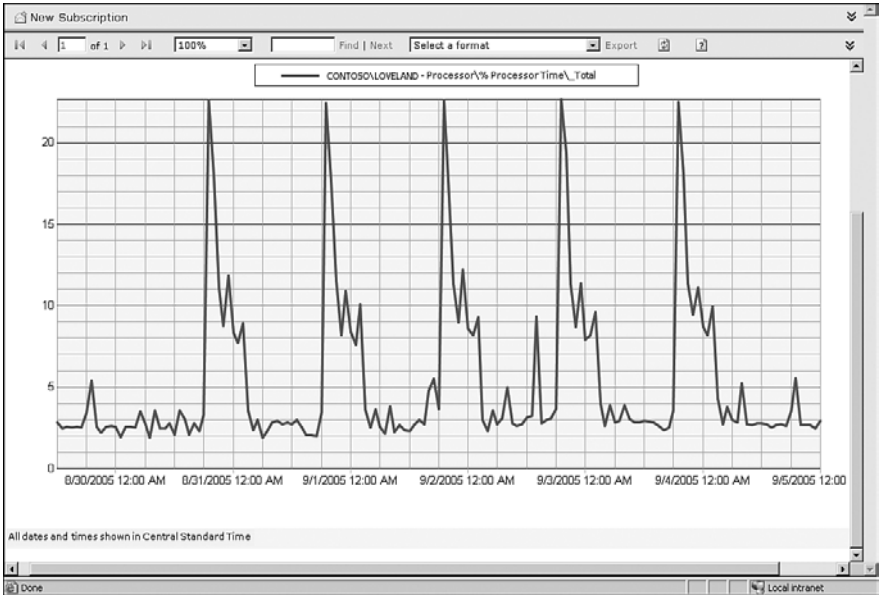


FIGURE 1.10 CPU performance report.

You can generate reports of the history of what has happened over any timescale where the data is collected to use with long-term trending and capacity planning. You can also look at the information being collected real-time, to get a snapshot view of what is happening within your organization and even drill down into the detailed specifics where needed.

MOM 2005 can also produce system and service availability reports to help keep the organization in line with SLAs. These reports can be an invaluable tool for managers to prove the value of IT initiatives or drive home the need for IT improvements.

This long-term view of information can be important for detecting trends and patterns that are otherwise hidden in a snapshot view of the information. Recall our previous example where the IT staff called out that CPU utilization was at 50%. With MOM in place, we can look at the historical information and see that this was actually a normal condition. Through the same process, we would be able to detect an increase in network utilization and diagnose the problem appropriately. With MOM on the job, the IT staff might not even need outside consulting services!

As might be expected, the amount of data collected from all these information sources can be massive. To handle this flood of data, MOM uses the Microsoft SQL Server database platform for centralized storage of data. Microsoft supports this MOM database storing up to 30GB of information for reporting on current and historical events, performance monitoring, and availability.

Over time, even with a large data store the information builds up and can fill up MOM's operational database. To keep MOM responding quickly, the capacity is included to utilize an archive database to move older data out of this system while still allowing it to be accessible for historical reporting and long-term trend analysis. The archive system can have larger and slower storage associated with it to help reduce costs. The system can even be placed on a completely different server if needed, which typically is recommended. Access to historical information is invaluable for a system administrator trying to understand what his servers, services, and applications are really doing.

Expertise

Immediately after installation, MOM is ready to go to work with built-in expertise. Using a comprehensive set of predefined rules that form an expert system, the system alerts you to significant events, suppresses unimportant events, and correlates seemingly unimportant events to understand underlying potential problems. Rather than simply collecting everything for the administrator to sort out, MOM uses built-in knowledge to decide what is important and what's not and escalates as needed. When it determines something is important, MOM alerts appropriate personnel that you identify. Before escalating to a live operator, it can even automatically respond to various events, such as restarting services. This is done using management packs, which are a system of rules and collections of rules.

Management packs contain the knowledge, in essence the gray matter, from Microsoft's best people. These include the product support teams, developers, and vast resources of

TechNet, Microsoft's technical database. This expertise is enhanced with the local expertise within your organization. Knowledge is added as events are alerted, troubleshooting is performed, and problems are resolved, thereby enhancing the system. Just like a human expert, MOM improves its skills and capabilities over time. After alerting the appropriate personnel, MOM assists in resolving the problem by providing detailed knowledge about the event, historical performance and event information, suggestions for fixes, and pointers for where to research further.

As shown earlier in the detail pane in the lower part of Figure 1.8, the highlighted alert contains concrete and specific guidance on what the alert means, the possible causes, possible resolutions, and where to get additional information if needed. The detail pane does not show the entire contents of the knowledge for this particular alert, so we duplicate the full text of the product knowledge section in the following sidebar. While in the console, you could click on the View button in the lower part of the screen in Figure 1.8 to launch a window with the product knowledge text in it.

Management Pack Knowledge

Summary

Pages/sec is the rate at which pages are read from or written to disk to resolve hard page faults. This counter is a primary indicator of the kinds of faults that cause system-wide delays since hard page faults, as opposed to soft page faults, require disk access.

This rule will generate an alert when the Pages/sec exceeds the defined threshold for a sustained period of time (Default: Memory\Pages/sec > 50).

When this performance threshold has been exceeded it often means that the system is low on physical memory because the operating system is reading from the hard disk to recover information from virtual memory. When a system is in this state, overall system performance is significantly diminished. This results in poor operating system and application performance.

Note: This rule requires threshold tuning before it can be used. As a result, the rule is disabled by default. Before enabling this rule, create a baseline Pages/sec performance signature for each system. After you have created a baseline, set a default threshold that will work for the largest percentage of managed nodes and then use the Overrides feature to define thresholds for exception cases.

Causes

The volume of Pages/sec can become high under the following circumstances:

- The computer has insufficient volume of Physical Memory.
- Too many applications that tend to use Virtual Memory are running simultaneously on the computer.

Resolutions

To confirm that excessive paging is occurring, add the Avg. Disk sec/Transfer (a physical disk counter) and Pages/sec counter values. If the product of these counters exceeds 0.1, paging is taking more than 10 percent of disk access time. If this occurs over a long period this can often be resolved by adding more memory to the computer.

To check for excessive paging that is due to the behavior of the applications that are running on the computer follow these steps. If possible, stop the application with the highest working set value, and see if that dramatically changes the paging rate. If you suspect excessive paging, check the Pages/sec counter in System Monitor. This counter, which is part of the Memory object type, shows the number of pages that had to be read from disk because they were not in physical memory. (Notice the difference between this counter and Page Faults/sec, which indicates only that data was not immediately available in the specified working set in memory.)

External Knowledge Sources

Sample Event

Other Information

Counter Type: Interval difference counter (rate/second)

Description: Memory\Pages/sec is the rate at which pages are read from or written to disk to resolve hard-page faults. This counter is a primary indicator of the kinds of faults that cause system-wide delays. Memory\Pages/sec is the sum of Memory\Pages Input/sec and Memory\Pages Output/sec.

Measurement Notes: Memory\Pages/sec is the number of pages read from the disk or written to the disk to resolve memory references to pages that were not in memory at the time of the reference. This is the sum of Memory\Pages Input/sec and Memory\Pages Output/sec. This counter includes paging traffic on behalf of the system Cache to access file data for applications. This is the primary counter to observe if you are concerned about excessive memory pressure (that is, thrashing), and the excessive paging that may result. This counter, however, also accounts for such activity as the sequential reading of memory mapped files, whether cached or not. The typical indication of this is when you see high number of Memory\Pages/sec, a "normal" (average, relative to the system being monitored) or high number of Memory\Available Bytes, and a normal or small amount of Paging File\% Usage. In the case of a non-cached memory-mapped file, you also see normal or low cache (cache fault) activity.

Performance: Memory\Pages/sec is a primary indicator used to determine if physical memory is a potential bottleneck.

Capacity planning: Watch for an upward trend in the value of Memory\Pages/sec. Add memory when paging operations absorb more than 20 to 50 percent of your total disk I/O bandwidth.

Operations: Excessive paging can lead to slow and erratic response times. Excessive paging can usually be reduced by adding RAM.

Alert Threshold: You should set an alert for when the value of Pages/sec exceeds 50 per paging disk.

As issues are resolved, MOM learns over time and builds that experience into its knowledge base. When the same type of event happens again, MOM is ready to provide the knowledge of what happened before and how it was resolved.

MOM also leverages other tools and technologies such as the Microsoft Baseline Security Analyzer (MBSA). The MBSA Management Pack conducts a routine scheduled security analysis to determine patch status, service pack status, and vulnerability status of all systems monitored by MOM. Figure 1.11 shows the results of a recent scan, indicating that service packs are up-to-date. However, a patch is missing, and there are several vulnerabilities in the Internet Information Services, Windows, Internet Explorer, and SQL Server configurations. For the SQL subsystem (on Fountain) in particular, the scan detected blank or simple passwords on 13 of 94 SQL logins.

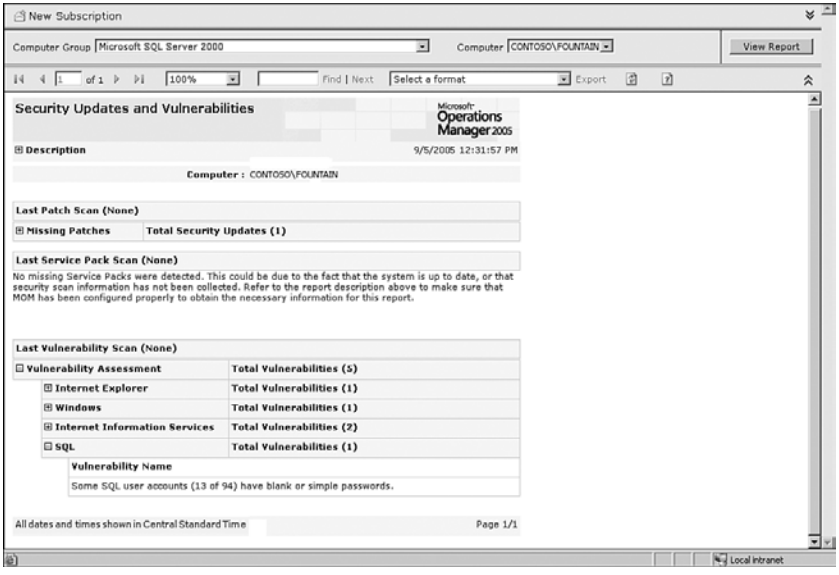


FIGURE 1.11 Security updates and vulnerabilities report.

This type of detailed and specific information is invaluable to IT professionals and security officers. Look back at Figure 1.10, which shows a New Subscription option in the upper left-hand corner. You can subscribe to any report, which generates the report automatically based on a user-specific schedule. The report is emailed or posted to a file share. The report format can be an Adobe Acrobat PDF, Excel, TIFF image, or XML file. You can even simply email a link to the report so that the information will generate at the time the user views the report. For security information, companies typically email reports in PDF format to the security officer on a daily basis.

Catching Missed Events

MOM monitors all the time, helping to make sure that no events are missed. More importantly, the system understands that certain events should take place and can alert if those events do not occur. MOM uses a special type of rule that checks for a condition to occur within a given time frame, such as every day between 1:00 a.m. and 5:00 a.m. If the

condition does not occur within that time frame, an alert is generated. This helps you catch an alert on problems such as missed backups. Still, MOM needs to be told to watch for the event; otherwise, it can't catch what it isn't looking for.

Reduced False Alarms

To reduce false alarms, MOM uses the built-in knowledge and correlates different types of events to make sure that it alerts when needed, which typically reduces the number of alerts to a fraction of the event count. This capability reduces the flood of information a typical management system generates, allowing you to focus on what is important to keeping your system up and performing at its best.

For example, Figure 1.12 shows an IIS log (file ex040829.log in Notepad) indicating that there was a variant of the NIMDA virus attack on the web server at 23:12:11 on 08/29/2006. However, the server is protected from such attacks by Microsoft service packs and security patches, as is indicated in the Security Updates and Vulnerabilities report. Therefore, the local agent on the computer simply raises the event as a warning that an error occurred, as can be seen in the Operations console in the background of Figure 1.12.

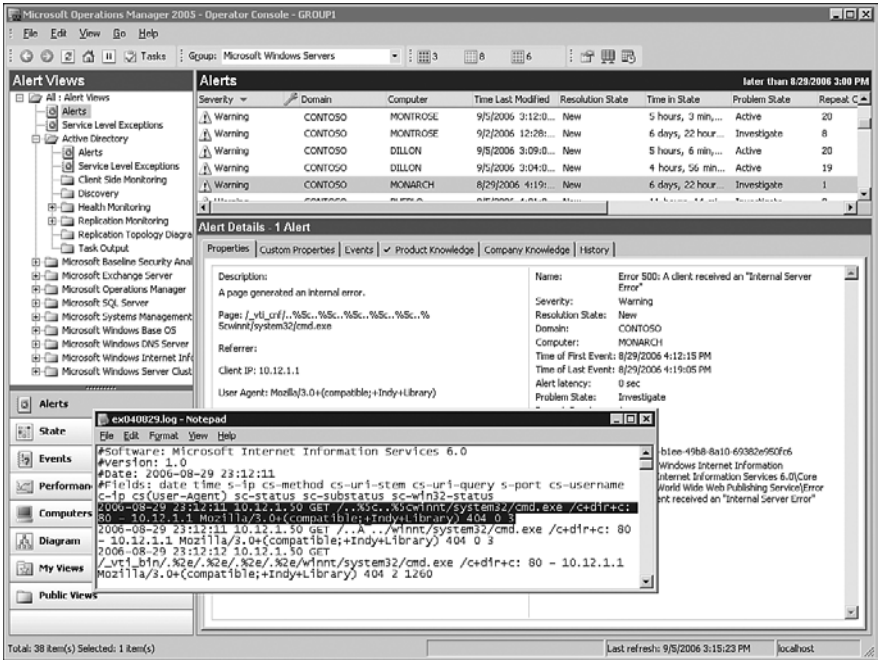


FIGURE 1.12 NIMDA virus attack event.

In this example, the administrators would not be responding to a false alarm. MOM, by default, only raises a warning on this type of event and allows you to report on the number of occurrences for analysis purposes. Alternatively, the rule could be tuned to a

higher level of severity on the event rather than just a warning and could notify the administrator of the attack.

MOM does all of this easily and automatically. MOM has the capability to automatically scan the network and install agents without any administrative intervention (although this is not turned on by default). Agents, rules, and management packs are updated and distributed automatically, helping you deploy your management infrastructure quickly and effectively. Using a central console, MOM allows you to implement a consistent systems monitoring and alerting policy to all systems in your organization. MOM deploys the agent needed to do the monitoring and the business logic that goes with it, automatically updating the appropriate systems with the appropriate business logic. It will even automatically remove business logic rules and the agent from the distributed systems, as appropriate.

MOM is also scalable to all sizes of organizations, performing well even as it scales. The same product and basic architecture can be used to support small, medium, and large organizations with their varied requirements:

- It works well for small organizations, where the requirements' focus might be on keeping costs low. In this case, you can install everything on a single box and have the capacity to monitor up to 50 systems.
- It works for medium-sized organizations, where fault tolerance and performance might be critical factors in the requirements. In this case, MOM supports redundant and load-balanced components to ensure that it can monitor hundreds of systems with no loss of performance or service.
- It also works well for large organizations, where fault tolerance, performance, and organizational divides must be bridged. MOM supports alert forwarding with bidirectional resolution and a hierarchical architecture to handle a large organization's requirements, in addition to its redundant and load balancing requirements. Moreover, while scaling, it still provides the cohesive view needed for a centralized management model.

Operations can be monitored through a console or a web interface. The consoles have views into the collected information, be it events, alerts, performance, or combination of all of the above. You can also view reports either through the consoles or published on a website. You can even view the status of your IT systems in a graphical diagram view that rapidly shows you the status of all systems, as in Figure 1.13. The highest-level state will be shown in the state of the group, shown in the center of Figure 1.13. In this particular example, the highest-level state is Error.

MOM 2005 can be deployed in small organizations, large enterprises, and anything in between. MOM's flexibility also allows you to start small, managing a specific group of servers, a department, or a specific application such as Exchange. After getting comfortable with the management platform, you can then scale it up to the rest of the organization.

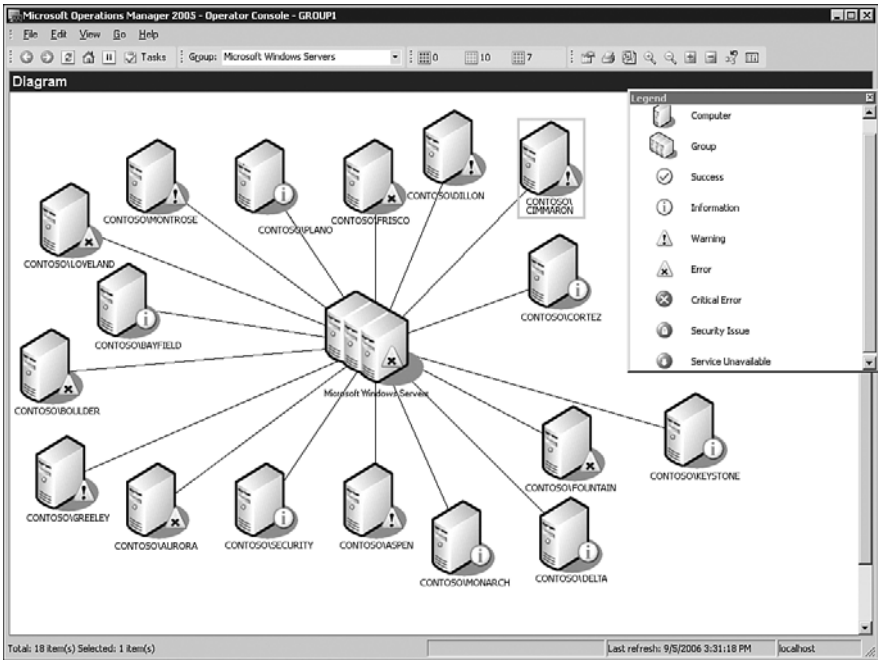


FIGURE 1.13 Diagram view with status.

With MOM handling your monitoring needs, you as an operations manager can relax (somewhat!) knowing that you will be alerted when there is a problem and have help in resolving it. It is like having an IT genie on the job 24x7! But it won't take your job, not if you read this book.

Microsoft System Center

Beginning with MOM 2005, Operations Manager is aligned with System Center. System Center is an umbrella or brand name for Microsoft's Systems Management family of products, and as such will have new products and components added over time. System Center represents a means to integrate system management tools and technologies to help you with systems operations, troubleshooting, and planning. Initial representatives of the System Center family include SMS 2003, MOM 2005, and System Center Data Protection Manager 2006; 2006 additions included System Center Reporting Manager 2006 and System Center Capacity Planner 2006.

Reporting and Trend Analysis

System Center Reporting Manager consolidates change and configuration information from SMS 2003 with event and performance information from MOM 2005, giving easy access to operational reports for managing your enterprise. If you are using both products, System Center provides additional reports correlating how changes in your SMS environment are affecting your system and service availability.

The data gathered by MOM is collected in a data warehouse, enabling many event, alert, and performance reports to be viewable from a web browser. The MOM reporting function uses Microsoft SQL Server Reporting Services, enabling organizations to easily create their own customized reports using Visual Studio. Reports can also be exported to multiple file formats (including Microsoft Excel, Adobe Acrobat, HTML, TIFF, CSV, and XML), and produced and delivered on a scheduled basis. Approximately 200 reports are available out of the box with MOM 2005. All data currently used with MOM Reporting will be in the System Center Reporting Manager.

Capacity Planning

System Center Capacity Planner is designed to provide tools and guidance required to efficiently create the architecture of a successful deployment, while also incorporating hardware and architecture "what-if" analyses for future planning. The Capacity Planner's initial scope assists with planning deployments of MOM and Exchange Server.

The Capacity Planner creates models with information on topology, hardware, software, and usage profiles. Further, it allows you to run simulations on the models for performance information. Capacity Planner ties into the DSI strategy by identifying when systems deviate from a defined performance model, providing guidance to correct those variations.

The Value Proposition of MOM

The value of MOM lies in three areas:

- Increasing the quality of service that IT departments deliver to their business units
- Reducing the operational cost to deliver that service
- Delivering a best-of-breed tool for Windows Management

As an events and performance management tool, MOM 2005 is designed to be a best-of-breed monitoring solution for the Windows Server platform, providing enterprise scale and event performance management. By incorporating a rich application and service monitoring environment using its management packs, MOM provides a high level of automation.

As an enterprise-ready solution, MOM provides redundant support and high availability with an open architecture—a requirement for computing enterprises that encompass multiple environments that include the use of non-Microsoft platforms. MOM is extensible, so it can integrate with other computing environments including third-party management suites such as Tivoli's TEC, HP OpenView, and the HP Network Mode Manager. In addition, the MOM-to-MOM Product Connector offers connectivity between multiple management groups for a multilayered hierarchical monitoring approach.

MOM 2005 can monitor, manage, and secure a wide range of resources, including computers, applications, server farms, e-commerce sites, and corporate servers. MOM

supports networked systems scaling up to thousands of computers on the network. MOM can continuously monitor user actions, application software, servers, and desktop computers running Microsoft Windows 2000 Server or later. (MOM 2005 can also provide limited monitoring of Windows NT4 systems.)

The goal for the IT manager considering MOM is to lower the cost of deploying and managing Windows solutions. This goal includes the "time to resolution"—or how quickly can the IT manager get an understanding of what is happening in the operating environment and then automatically (or as quickly as possible) be able to achieve a resolution. MOM (when correctly tuned) is positioned to help you tame this fire hose (as shown in Figure 1.14) and control the deluge of system and operational information pouring at you from across your operating environment and is a key component of DSI.

FIGURE 1.14 Taming the fire hose.

Out of the box, MOM hits the ground running by supporting key applications such as Microsoft Exchange and Active Directory. It comes with a comprehensive set of rules, alerts, knowledge, reports, views, and responses built into the product, requiring little or no configuration or setup for the majority of applications.

MOM's huge body of expertise solves one of the major obstacles that many enterprise management solutions encountered prior to MOM. Most of the big framework management platforms, such as TNG Unicenter, HP OpenView or Tivoli TEC, provide an infrastructure that has the potential to do great things and are sold based on that potential. Then after a company has spent mucho dollars to deploy the infrastructure, the hard work of configuring the product starts. Sometimes, due to the difficulty of configuration, the plug is pulled on the framework products, which leaves a bad taste in the mouth of the company after apparently wasting its money.

MOM completely changes the paradigm by shipping the product with the vast majority of the configuration done for you. This instant return on investment provides a huge win when the system starts detecting operational problems, alerting the appropriate personnel, resolving issues, and providing extensive reports with little or no IT effort.

Summary

This chapter introduced you to operations management. You learned that operations management is a process to enhance the supportability of a production environment. The chapter illustrated how MOM can solve a horde of problems. MOM works to eliminate the islands of information in your shop, notifies you of problems, and maintains a historical database of what happened and how issues were resolved.

We discussed ITIL, an international set of best practices for IT Service Management, which describes at a high level what should be accomplished, although not actually how to accomplish it. In furtherance of that process, Microsoft chose ITIL as the foundation for its own operations framework. With the MOF, Microsoft provides both descriptive (what to do and why) as well as prescriptive (how to do it) guidance for IT service management.

Microsoft's management approach, which encompasses MOF and also DSI, is a strategy or blueprint intended to automate data center operations. Microsoft's investment in DSI includes building systems designed for operations, developing an operationally aware platform, and establishing a commitment to intelligent management software.

MOM is a tool for managing the Windows platform to increase the quality of service IT delivers while reducing the operational cost of delivering that service. Together with SMS and the System Center products, MOM is a key player in Microsoft's approach to system management.

Management software has become a key element in Microsoft's strategy to convince corporate customers that Redmond is serious about proactive management of Windows systems. As we step through the different areas of this book, you'll become aware of just how powerful MOM is, and how serious Microsoft is about operations management.

This page intentionally left blank

CHAPTER 2

What's New

IN THIS CHAPTER

- The History of MOM
- MOM 2000 Versus MOM 2005
- Using MOM 2005 Workgroup Edition

Now that you've had an introduction to the concepts behind operations management and the capabilities of Microsoft Operations Manager (MOM), we are ready to focus on the differences in various versions of MOM. We will look at what has changed between MOM 2000 and MOM 2005, including changes to component functionality, changes in terminology, consoles, a revamped reporting feature, and increased capacities with the new version. We will also take a look at MOM 2005 Workgroup Edition, discussing its capabilities and the differences between the Workgroup Edition and full version of MOM 2005.

The History of MOM

First, let's spend a moment on a brief history regarding Microsoft's entry into the server monitoring marketplace. Microsoft began including server health and monitoring functions with Microsoft Application Center 2000, Systems Management Server (SMS) 2.0, and BackOffice Server 2000. The capability enabled a system administrator to have a centralized view of information pertaining to functional health, performance, and event log data of the servers used within that specific application server environment.

Microsoft Operations Manager was originally based on technology developed by Mission Critical Software, which Microsoft licensed in 2000. Microsoft's first release of the management software addressed scalability and performance issues, along with significant improvements to management packs for Microsoft applications software. With an oft-stated goal of making the Windows Server platform more manageable, Microsoft positioned MOM 2000 as an enterprise monitoring solution including comprehensive event management, monitoring and alerting, reporting, a built-in knowledge base, and trend analysis capabilities.

Happy Mom's Day, Microsoft!

Just in time for Mother's Day in May 2001, Microsoft launched its operations management product, known as MOM 2000.

Some Acquisition Trivia

A question typically asked in every major software development project is whether to build the application in house or buy it from others. In October 2000, Microsoft and NetIQ Corporation announced a technology licensing agreement and partnership in operations management, where Microsoft licensed NetIQ's Operations Manager technology—newly acquired by NetIQ with its recent merger of Mission Critical Software—for managing the Windows 2000 environment and later versions of Windows. The agreement between Microsoft and NetIQ also included a three-year technology partnership to jointly develop management software for Windows 2000 and other servers.

For those of you who are really into factoids, Mission Critical Software also was responsible for the technology that became the basis of Microsoft's Active Directory Migration Tool (ADMT). Stephen Kangas, Vice President of Strategic Alliances at Mission Critical Software prior to its merger with NetIQ, was behind the technology license and development agreement pertaining to ADMT and also facilitated the Microsoft/NetIQ Operations Manager licensing agreement. Stephen later retired from NetIQ Corporation and joined Tidal Software as Senior Vice President of Strategic Alliances.

During the MOM 2000 life cycle, a single service pack was released. MOM 2000 Service Pack 1 included globalization, support for the MOM database on failover clusters, a number of performance improvements to the event management infrastructure, enhancements to most of its management packs with particular emphasis on those for Microsoft Exchange Server and Active Directory monitoring, and several new management packs. Continuing development of the product, Microsoft began work in late 2003 on the next version of MOM. Microsoft Operations Manager 2005 was released in September 2004. MOM 2005 Service Pack 1 was released in July 2005, and work is underway for System Center Operations Manager 2007, Microsoft's next version of Operation's Manager. Figure 2.1 illustrates the MOM life cycle.

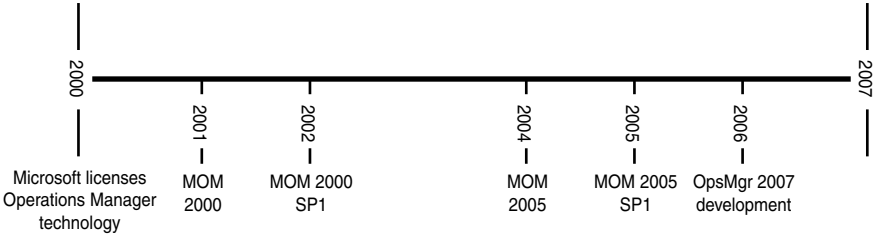


FIGURE 2.1 MOM development timeline.

MOM 2000 Versus MOM 2005

MOM 2005 is more an evolutionary than a revolutionary change from MOM 2000. Along with enhanced scalability, some major improvements were made in the user interface as well as in reporting capabilities. Additionally, Microsoft has reworded some of the terminology and rearchitected several of the roles; so if you are a MOM 2000 administrator, it would be useful to understand these changes as part of planning your upgrade to MOM 2005.

Terminology Changes

A number of terms have changed between MOM 2000 and MOM 2005. MOM 2000 devotees will have to forget they knew phrases such as the DCAM, Consolidator, and configuration groups. This section gives you an overview of these changes, and Table 2.1 recaps these terms.

TABLE 2.1 Terminology Equivalents and Changes

MOM 2000 Term	MOM 2005 Term
Configuration group	Management group
Consolidator	MOM Server
DCAM	MOM management server
Master configuration group	Destination management group
OnePoint service	MOM service
Zone configuration group	Source management group
Agent Manager	Agents, MOM Server component

MOM Management Server

The MOM 2000 Data Access Server Consolidator Agent Manager (DCAM) has been renamed to *management server* in MOM 2005. You can have multiple management servers in a MOM 2005 management group. The management server consists of three components: the Data Access Server (DAS), the MOM Server, and the MOM agent, which we discuss in this chapter.

MOM Server

The Consolidator has been renamed the *MOM Server*. In MOM 2000, the Consolidator receives collected data from agents and sends that information to the Data Access Server (DAS). The Consolidator acts as an agent on the DCAM by performing all the actions that agents perform on remote computers. In MOM 2005, the MOM Server component replaces the Consolidator functions.

Management Group

In MOM 2005, the configuration group has been renamed to *management group*. A configuration group in MOM 2000 consists of a MOM database, one or more DCAMs, a MOM Administrator console, and one or more agents. Configuration groups are used to group

computers together, simplifying administration and also increasing the scalability of the MOM environment. In MOM 2005, a management group is made up of a MOM database, one or more management servers, one or more Administrator and Operator consoles, and one or more agents.

Source and Destination Management Groups

In MOM 2005, the zone configuration group is now called the *source management group*, and the master configuration group is now the *destination management group*.

In a MOM 2000 environment that has multiple configuration groups, zone and master configuration groups form a hierarchy in which alerts from one configuration group are forwarded to another. The sending configuration group is called the *zone configuration group*, which forwards its alerts to a *master configuration group*. This enables MOM 2000 to support multitiered configurations such that organizations with multiple locations could centralize alerting using a master configuration group. The names have changed in MOM 2005, but the functionality is the same. Figure 2.2 illustrates a multitiered example of management groups.

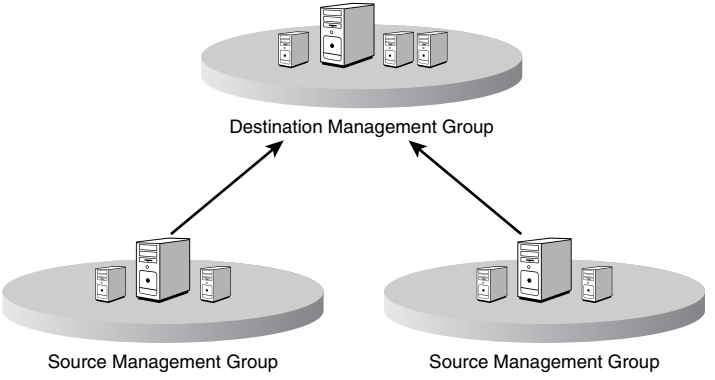


FIGURE 2.2 Multiple management groups.

MOM Service

The OnePoint service, which runs on the Consolidators and agents in MOM 2000, has been renamed the *MOM service*. In MOM 2005, the MOM service runs on the management servers and all agent-managed computers.

Functionality Changes

This section describes some of the changes in functionality implemented in MOM 2005.

DAS

The Data Access Server (DAS) is a Component Object Model Plus (COM+) application that manages access to the MOM database, OnePoint. One of the functions of the MOM 2000 Consolidator is sending data to the DAS, which adds all data to the database. The DAS

provides a communication interface between the OnePoint database and other MOM components, including the Consolidator, MOM Administrator console, and the MOM Web console.

In MOM 2005, the DAS performs the same role, but it now receives data from the MOM Server (rather than the Consolidator) and adds data to the MOM database. The DAS is responsible for controlling the flow of information between the MOM components, including the database and the MOM Server, Administrator, Operator, and Web consoles. Figure 2.3 illustrates the data flow of these components.

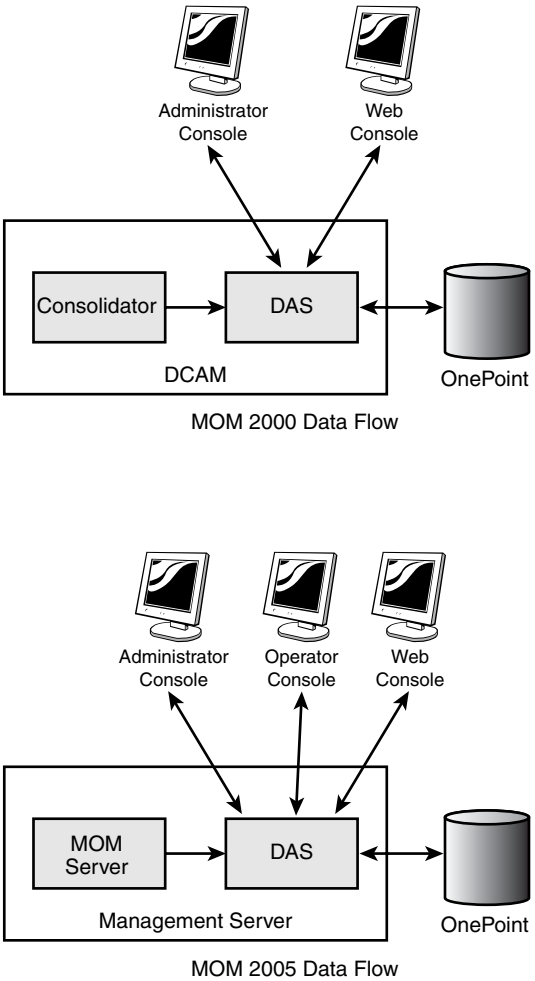


FIGURE 2.3 A comparison of the data flow in MOM 2000 and MOM 2005.

MOM Agent

The MOM agent is a component that monitors and collects data from a managed computer. In MOM 2000, all monitored computers have agent software installed on them. MOM 2005 additionally provides agentless monitoring, where the agent running on the management server collects data across the network from a managed computer. As described further in Chapter 9, "Installing and Configuring Agents," agentless monitored systems often have limited monitoring functionality compared to what is available with agent-managed systems.

Agentless Monitoring

Evaluate the use of agentless monitoring based on your own particular requirements. A number of management packs do not support agentless monitoring. Other issues associated with agentless monitoring include

- Performance overhead
- Bandwidth issues
- Firewall and port issues
- Numeric limitations on the number that can be deployed per management server and group

We discuss these topics further throughout this book.

Agent Manager

MOM 2000 relies on the Agent Manager for automated agent management, including discovery, determining computer group membership, scanning remote systems for computer attributes, and agent deployment. The Agent Manager uses remote procedure calls (RPC) for communications, which limits functionality across firewalls if the Agent Manager does not have administrative rights on the managed computer.

In MOM 2005, the Agent Manager no longer exists. The MOM Server role utilizes agents and tasks to perform self-management activities, including deploying agents, starting and stopping agents, and changing agent configurations. The agent on the managed computer now scans computer attributes and reports this information back to its management server.

DCAM Account Split into Management Server Action Account and MOM Service Account

The MOM 2000 Consolidator and Agent Manager share a service account, which requires local administrator rights on the DCAM and a domain account with administrative access on each managed computer. Additionally, that same account is used to access the Data Access Server (DAS), necessitating a single service account either to be a member of the Domain Admins group or to have local administrative permissions on the DCAMs, database server, and every managed computer.

In MOM 2005, the DCAM account becomes two separate accounts, which enhances the security of the MOM environment. These accounts are the MOM Service account and Management Server Action account:

- The *MOM Service account* uses the credentials of either Local System (Windows 2000) or Network Service in a Microsoft Windows Server 2003 environment. The Network Service account has a lower level of permissions than the Local System account, enhancing the security of the MOM service. The MOM Service account is responsible solely for communication between the agents and the management server.
- The *Management Server Action* account monitors the MOM Server itself, just like any other MOM agent. It is also the default account for installing and uninstalling remote agents. Local administrative access is required for agentless communication. If the account is used to install or uninstall agents, it also needs local administrative access to each server where it will install an agent.

Consoles

MOM 2000 has three consoles: the Administrator console, which is used for administration and operations; a web-based console showing open alerts; and a web-based Reporting console.

Administrator Console Becomes Administrator and Operator Consoles

In MOM 2005, the console used for administration and operations monitoring is split into two components: the Administrator console and the Operator console. The *Administrator console* is used for maintaining management packs and overall MOM administration. Figure 2.4 shows the MOM 2005 Administrator console for a newly installed management group that has had minimal configuration.

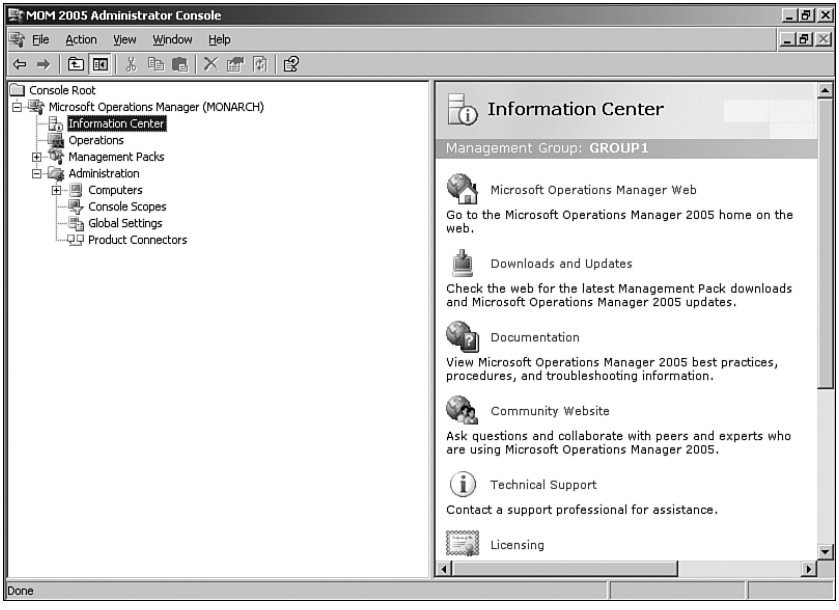


FIGURE 2.4 The MOM 2005 Administrator console MMC snap-in.

The second console is known as the *Operator console* and is patterned after the Microsoft Outlook 2003 user interface. The Operator console was developed based on feedback provided to Microsoft by MOM 2000 administrators. This console provides access to operations information such as alerts, events, performance data, views, tasks, and topology diagrams. Figure 2.5 shows the MOM 2005 Operator console. MOM supports a maximum of 15 active Operator consoles in a single management group.

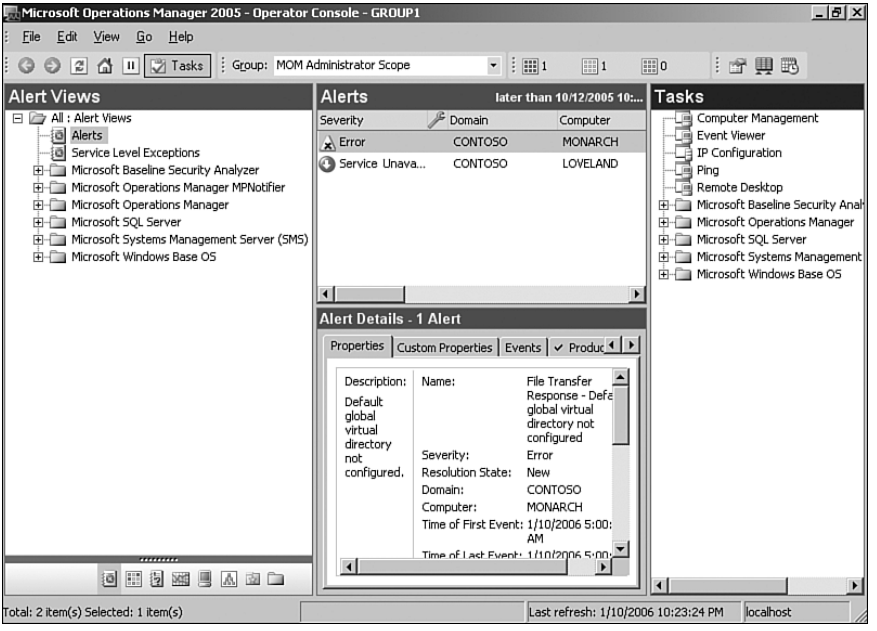


FIGURE 2.5 The MOM 2005 Operator console.

A nice visual enhancement in this console is the *state view*, which provides a roll-up status display that identifies servers with a red, yellow, or green icon to show at a quick glance the health of individual machines. If a yellow icon is associated with a server, the server's capacities are impaired, whereas a red icon indicates a severe problem. Glancing at the column headers in the console gives you an instant view of the condition of various services running on your network and enables you to drill down quickly to a problem area.

The Operator console also boasts a *diagram view*, which gives a graphical representation of the current state of health of monitored computers using the red, yellow, and green icons to indicate status.

Web Console

As in MOM 2000, MOM 2005 provides web access to operational data in a Web console. Be aware that the Uniform Resource Locator (URL) to access the MOM Web console has changed in MOM 2005. Whereas the previous address was *http://servername/OnePointOperations*, the new URL is of the format *http://servername:portnumber*, where

servername is the management server with the software loaded for the Web console, and *portnumber* is the default port number 1272. Figure 2.6 shows the Web console.

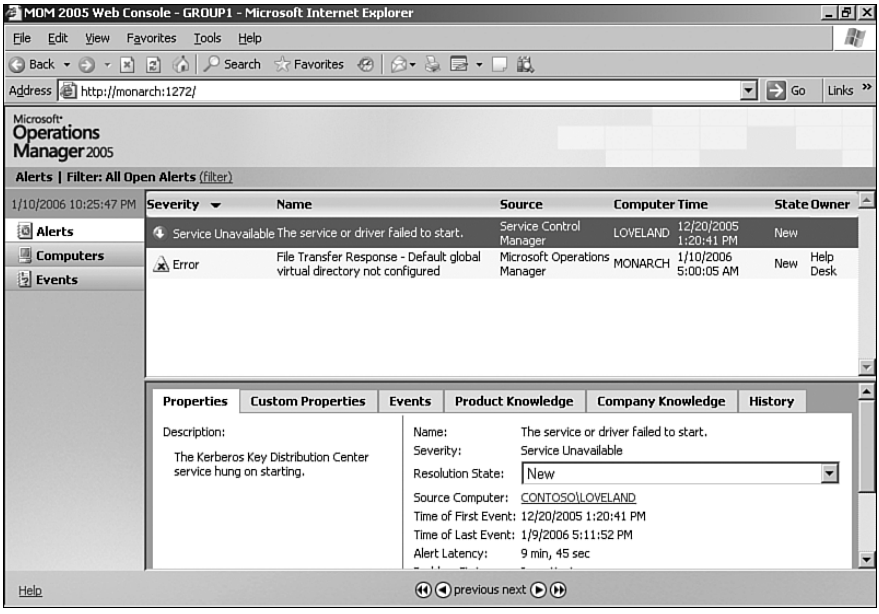


FIGURE 2.6 The MOM 2005 Web console.

Reporting Console

Shown in Figure 2.7, the MOM 2005 web-based Reporting console provides a front-end view into the MOM Reporting Server, enabling you to view event, alert, and performance reports using a web browser. Report data can be exported to other formats such as a Microsoft Office Excel spreadsheet. In addition to viewing reports immediately, you can subscribe to favorite reports and automatically receive new versions or have them distributed to individuals in your organization.

MOM Reporting

MOM Reporting, previously based on a Microsoft Office Access reporting system, now includes automated data warehousing and uses Microsoft SQL Server Reporting Services to generate reports. The Reporting database contains a copy of the operational data collected in the MOM OnePoint database, updated with scheduled nightly extractions. During the nightly import, historic data is moved from the operational database to the data warehouse.

Report templates are typically distributed with management packs. With SQL Server and SQL Server Reporting Services as the basis for MOM reporting, creating customized reports is greatly simplified in MOM 2005 because you can write queries using SQL Server Reporting Services to create new reports.

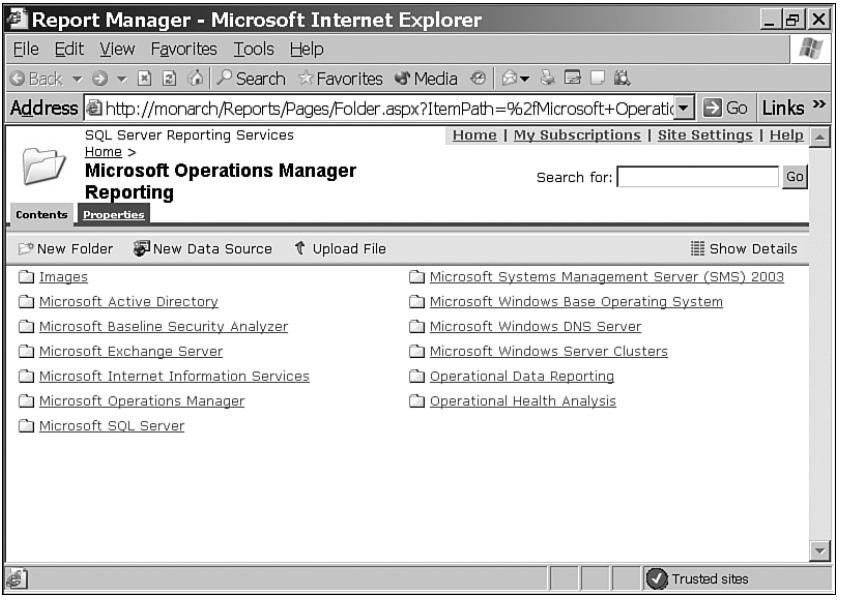


FIGURE 2.7 The MOM 2005 Reporting console.

Where Does the Data Go?

If the data transfer job does not successfully run, you are not able to view historic data in the MOM Reporting database. When the job is successful, the data is copied to the MOM Reporting database and then groomed from the Operational database.

Changes in Capacity

With the most recent version of MOM, Microsoft has increased capacity in several areas to extend MOM's monitoring capabilities. Table 2.2 compares MOM 2000, MOM 2000 Service Pack 1 (SP1), MOM 2005, and MOM 2005 SP1 management features. The terminology utilizes the MOM 2005 nomenclatures.

TABLE 2.2 Comparison of MOM Capabilities Across Versions

Feature	MOM 2000	MOM 2000 SP1	MOM 2005	MOM 2005 SP1
Managed computers in a management group	1,000	2,000	3,500	4,000
Managed computers per management server	700	1,000	1,200	2,000
Management servers per management group	4	10	10	10
Source management groups forwarding to a destination management group	6	10	10	10

Prerequisites

Table 2.3 compares the basic hardware and software requirements for both versions of MOM.

TABLE 2.3 Comparison of MOM Minimum Requirements Across Versions

Component	MOM 2000	MOM 2000 SP1	MOM 2005	MOM 2005 SP1
Processor	Pentium-compatible 550-MHz or higher	Pentium-compatible 550-MHz or higher	Pentium-compatible 550-MHz or higher	Pentium-compatible 550-MHz or higher
Memory	512MB of RAM	512MB of RAM	1GB of RAM if all components on a single server; otherwise 512MB	1GB of RAM if all components on a single server; otherwise 512MB
Hard disk	1GB plus 5GB for OnePoint	1GB plus 5GB for OnePoint	1GB plus 5GB for OnePoint, 200GB for MOM Reporting	1GB plus 5GB for OnePoint, 200GB for MOM Reporting
Operating System	Windows 2000 Server Family, SP2 or later	Windows 2000 Server Family, SP2 or later	Windows 2000 Server Family, SP 4 or later, or Windows Server 2003 Family	Windows 2000 Server Family, SP4 or later, or Windows Server 2003 Family (with SP1 for SQL Server 2005)
Database Server	SQL Server 2000 and Access 2000 or later for reporting	SQL Server 2000 and Access 2000 or later for reporting	SQL Server 2000, SP3a or later, and SQL Server 2000 Reporting Services for reporting	SQL Server 2000, SP3a or later, SQL Server 2005, and SQL Server 2000 Reporting Services with SP1 for reporting (or the SQL Server 2005 Reporting Services component)

The MOM 2005 Prerequisite Checker is a nice addition to the installation process, letting you know exactly what deficiencies you have before starting your MOM install. Requirements for MOM 2005 are further described in Chapter 6, "Installing MOM 2005."

Additional Enhancements

Some additional changes you will find in MOM 2005 include the following:

- **64-bit support**—Inclusion of a 64-bit agent to support managing applications running on Itanium-based 64-bit operating systems using Windows Server 2003.

- **Maintenance mode**—The capability to stop alerts from showing in the Operator console and needless notifications going out while a system is undergoing maintenance, which typically would generate a high volume of alerts.
- **Agentless monitoring**—Limited management capabilities to monitor a server without installing a MOM agent. This is described in detail in Chapter 9.
- **Rules override**—The capability within a Management Pack to override default parameters for selected computers or groups, including precedence setting to avoid potential conflicts from multiple overrides.
- **Multihoming**—The capability to take information collected by MOM agents and send it to multiple management groups. Multihoming is also described in Chapter 9.
- **Multitiering**—Support for bidirectional alert synchronization and aggregated views between tiered MOM servers in distributed environments. See Chapter 10, "Complex and High Performance Configurations," for additional information.
- **Full globalization**—MOM 2005 now operates in multiple languages and localized environments. MOM is localized for language usage in English, French, German, and Japanese.

Using MOM 2005 Workgroup Edition

Let's take a look now at MOM 2005 Workgroup Edition. New with this release of MOM, Workgroup Edition is targeted toward smaller Windows Server System-based environments with 10 or fewer servers. It is designed to simplify event management and alerting for small to medium-sized businesses.

Real World—Using MOM 2005 Workgroup Edition

A commonly seen implementation of MOM 2005 Workgroup Edition is to maintain separate MOM environments such as a demilitarized zone (DMZ) or environment where a separate group completely manages its own group of servers.

Workgroup Edition contains a subset of the capabilities available in the full implementation of MOM 2005. It includes the Administrator and Operator consoles, along with a web-based client interface. Workgroup Edition does not have reporting capabilities because it does not include support for SQL Server Reporting Services. The MOM Connector Framework is also not supported, so there is no capability for connecting to other MOM servers or other enterprise monitoring tools.

Workgroup Edition supports the no-charge Microsoft SQL Server 2000 Desktop Engine (MSDE) and its SQL 2005 counterpart, Express Edition (SQL Server 2005 requires MOM 2005 Service Pack 1), enabling you to save costs on the database software and pay a lower licensing fee for the monitoring software. If you want to use a server edition of SQL

Server, you can certainly do that as well. Workgroup Edition comes with preinstalled management packs, and its Operator and Administrator consoles have the same functionality as MOM 2005.

An Interesting Utility

Along with MOM 2000, Microsoft also provided a Resource Kit and a Software Development Kit (SDK). An interesting utility released with the MOM 2000 Resource Kit was the MOM Server Status Monitor, or SSM. The SSM provided a simple dashboard-type interface to enable administrators to quickly view the "up or down" status for as many as 10 servers, without the need for installed agents. It was, in other words, a rather lightweight mode of operations monitoring for smaller environments—conceptually a precursor to MOM 2005 Workgroup Edition.

Workgroup Edition runs on Windows Server 2003 in an Active Directory environment and can manage both Microsoft Windows 2000 Server and Windows Server 2003 systems. The full list of monitored systems for Workgroup Edition includes the following:

- Microsoft Windows NT Server 4.0 with Service Pack 6 (agentless monitoring only)
- Microsoft Windows 2000 Professional with Service Pack 4 or later
- Microsoft Windows 2000 Server with Service Pack 4 or later
- Microsoft Windows 2000 Advanced Server with Service Pack 4 or later
- Microsoft Windows 2000 Datacenter Server with Service Pack 4 or later
- Windows XP Professional with Service Pack 1 or later
- Windows Server 2003, Standard Edition, with Service Pack 1 or later
- Windows Server 2003, Enterprise Edition, with Service Pack 1 or later
- Windows Server 2003, Datacenter Edition, with Service Pack 1 or later

Should you decide after using Workgroup Edition that you want to use the full-flavored MOM 2005, an upgrade process is supported, which is described in Chapter 7, "Upgrading to MOM 2005."

The capabilities of MOM 2005 not available in MOM 2005 Workgroup Edition are the following:

- Reporting console
- SQL Server Reporting and Reporting database
- MOM Connector Framework
- Bidirectional multitiering
- Software assurance

The significant features available in both editions include the capabilities listed in Table 2.4.

TABLE 2.4 Features Available in MOM 2005 and MOM 2005 Workgroup Edition

Function	Component
Event monitoring	Maintenance mode
	Event overrides
	Auto-alert resolution
	Instance-aware monitoring
	State monitoring
	Topology monitoring
User Interface	Administrator console
	Web console
	Event view
	Attribute view
	Computer view
	Computer Group view
	Performance view
Operations	Nested computer groups
	Dynamic computer groups
	Tasks
Management Pack functionalities	Service and instance aware
	Service discovery
	Cluster monitoring
	Tasks and diagnostics
	Overrides
	Responses before alert suppression
	Command-line Import/Export tools
	Rule group versioning
Deployment	Agentless monitoring
	64-bit agent support
	Internationalization
	Firewall support
	Server discovery wizard
Security	Scopes of administration
Infrastructure	Cluster support
	Administrative partitions
Performance	System discovery time
	Agent footprint
	Agent installation time

Online Comparison Matrix

For an online comparison between MOM 2005 and MOM 2005 Workgroup Edition, see http://go.microsoft.com/fwlink/?LinkId=50016.

Discussions throughout this book refer to the full version of MOM 2005, rather than Workgroup Edition, unless otherwise specified.

Obtaining Trial Versions

Trial versions of both the Workgroup Edition and the full version of MOM 2005 are available for 120 days and can be downloaded from the Microsoft Download Center at the following locations:

http://go.microsoft.com/fwlink/?LinkId=50017

http://go.microsoft.com/fwlink/?LinkId=50018

Summary

In this chapter, we discussed the differences between MOM 2000 and MOM 2005. We covered changes in terminology, consoles, reporting, and capacity. We also introduced MOM 2005 Workgroup Edition and compared the features of Workgroup Edition with the full version of MOM 2005. Workgroup Edition is new with MOM 2005.

The next chapter talks about how MOM works; it includes an architectural overview and discussion of key components within MOM 2005.

This page intentionally left blank

CHAPTER 3

How Does It Work?

IN THIS CHAPTER

Successfully deploying Microsoft Operations Manager (MOM) 2005 requires understanding how it works and how to implement it. MOM 2005 is a powerful tool, but that power comes at the expense of a certain amount of complexity. In this chapter, we continue our introduction to MOM 2005 with an architectural overview and discussion of some of its major components. We discuss several MOM components including agents, the MOM Service, and the Data Access Service.

You'll become familiar with terms such as management group, management server, managed computer, and management packs. If you have already read Chapter 2, "What's New," you may notice that some of these components were previously introduced as new functionality with MOM 2005. This chapter provides the groundwork for understanding MOM, which will assist in planning your installation and deployment of MOM.

Architectural Overview

MOM obtains raw event and performance data to translate into system health information. Using rules, which are MOM's basic unit of instruction, you can define the characteristics of a properly running application and have MOM warn you when these capabilities are not being met. MOM collects event and performance data on monitored systems, looking for specific events that indicate poor performance, errors, or other factors specified in its rules.

MOM not only collects data, it filters that information so that you see only what is important. MOM also consolidates multiple occurrences of events into a single representation—minimizing superfluous "noise" and data. Alerts occur when specific events or performance conditions occur.

Monitoring begins after installing one or several management groups, importing management packs, enabling rules, and identifying computers to monitor. The monitored computers

send event and performance data to a management server, which stores that data in the MOM database. Operational data is viewed using the MOM Operator console or a web-based console. Data can also be maintained in a reporting database for long-term analysis and study.

What Is a Management Group?

The basic management unit of MOM is the MOM *management group,* illustrated in Figure 3.1. A management group is a MOM installation that includes one MOM database, one or more MOM management servers, and MOM agents installed on monitored systems. You can optionally install a Report server, Reporting database server, and/or additional management console(s). MOM can also manage a limited number of computers using an agentless monitoring technique.

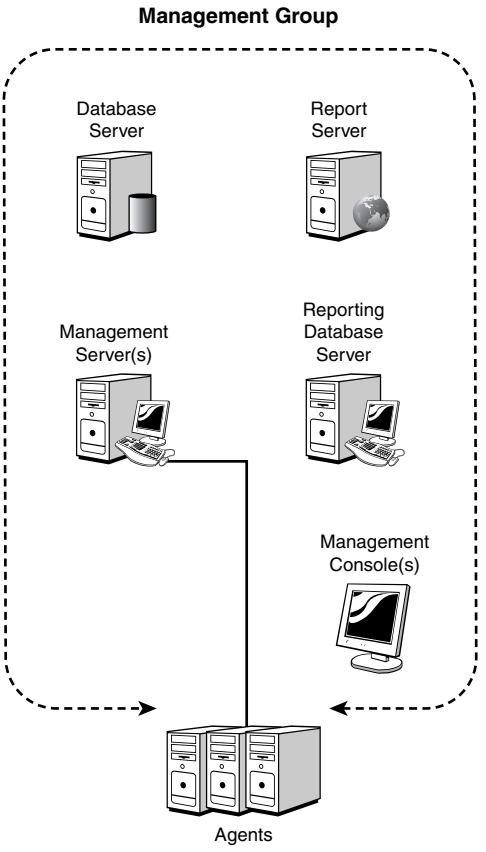


FIGURE 3.1 The MOM management group.

Management Group Names

A management group is identified by a unique alphanumeric name, which is specified when you install a management server. The management group name cannot be

modified after the management server is built; changing the name requires removing all MOM components and reinstalling them. The group name is up to you, although it is often advantageous to base them on geographical locations, organizational departments, or administrative needs.

The management group provides the features and benefits discussed in Chapter 1, "Operations Management Basics," namely:

- Event-based monitoring
- Easily deployed and scalable infrastructure
- Effective system availability and performance tracking

There are quite a few MOM components, all of which are ultimately bound into a management group. A functional management group contains the following components:

- Operations database
- Management Server
- Data Access Service (DAS)
- Agents
- Administrator console
- Operator console

There are optional components, including:

- Reporting database
- Reporting console
- Web console

In the next section we look at these components and how they interoperate.

Server Roles

The MOM components can be grouped into server roles (shown in Figure 3.2), which is ultimately what is built during your MOM implementation. The standard component groupings are

- **Database server role**—The database server normally contains the operations database and is a platform optimized for data collection—that is, to rapidly process a large amount of incoming data from the management servers. In classic client server architecture, this is known as the *backend tier*. In the MOM architecture, the database server is a big portion of the data layer or tier.

- **Management server role**—The management server typically contains the MOM service, the DAS, an agent, the Administrator console, the Operations console, and the Web console. The management server handles most of the centralized business logic and presentation layer functions, with the important exception of the reporting functions.
- **Report server role**—The report server typically contains the reporting database and the Reporting console. The reporting database is frequently located on a separate server for performance reasons. Using a separate server allows large volumes of data to be retained and mined with the reporting function, without affecting the operation's function on the database and management servers.

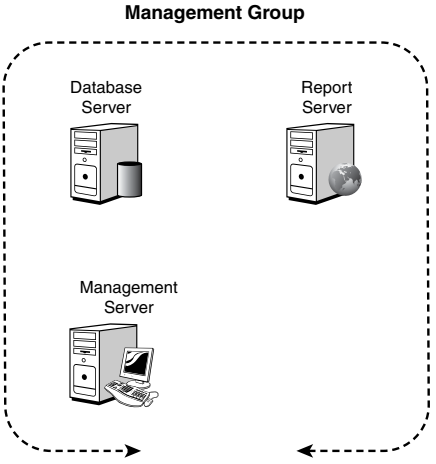


FIGURE 3.2 Management group roles.

In any given MOM installation, you can combine these roles in a variety of ways. In smaller installations, the server roles might all be on the same physical server with the net effect that there is only one "MOM Server." In a medium-sized organization, there might be two physical management servers for fault tolerance and a single database server with both the operations and reporting functions. In a large enterprise organization, there would likely be separate physical servers for the database server and the reporting database server, as well as multiple management servers for both load balancing and fault tolerance (and possibly also clustering the databases). Chapter 4, "Planning Your MOM Deployment," covers the rationale for splitting or combining the roles, as well as how to create a MOM 2005 design that meets the needs of your organization.

A management group can have multiple management servers as shown in Figure 3.3. Reasons for having multiple management servers include:

- Scalability
- Fault tolerance
- Security
- Crossing geographic or network boundaries

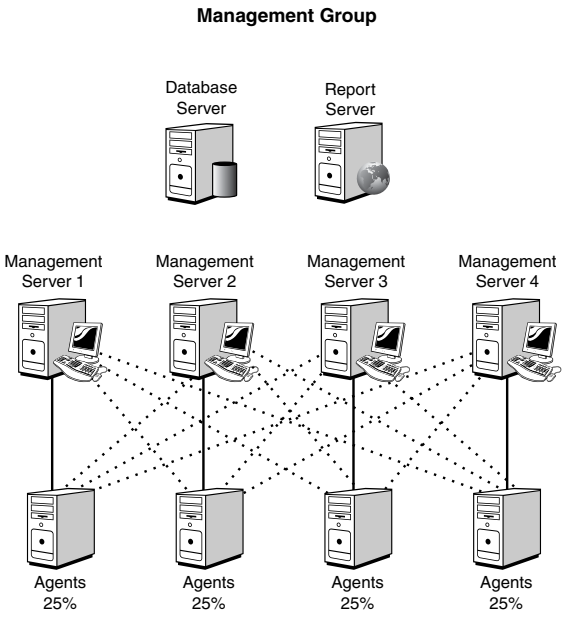


FIGURE 3.3 Management group with four management servers.

Agents within the management group have a primary management server assigned to them, and then each of the remaining management servers are backup management servers for the agent. Figure 3.3 shows four management servers with each assigned 25% of the agents, represented by the solid lines. The mesh of dotted lines represents the redundant failover connections the agents are automatically configured to use. Agent configurations are dynamically adjusted as new management servers are brought online or decommissioned. In the event that an agent fails over to one of its backup management servers, it periodically checks to see whether its primary management server is back online and fails back automatically when that occurs. More information on failover processing is available in Appendix A, "MOM Internals."

Communications

As you can see in Figure 3.4, MOM uses a variety of communications methods that are optimized for security and efficiency. Notice that the communications between the management server and the agent are different depending on the direction of the communication. This has important ramifications for firewall support and security, which we will discuss later in this section.

For the Remote Procedure Calls (RPC)/Distributed Component Object Model (DCOM) protocols, RPC uses Transmission Control Protocol (TCP) port 135, and DCOM uses a nightmarish combination of TCP, User Data Protocol (UDP), ports, and connections.

DCOM is particularly troublesome for firewall access because it dynamically assigns ports to processes. By default, it freely assigns TCP and UDP ports ranging from 1024 to 65535, making it difficult to function securely across a firewall. In addition, new connections are established when responding to a client, meaning that the port the client used for the request is not the same as the port used for the response. Also, DCOM does not support Network Address Translation (NAT), which is among the more common methods of configuring a firewall. You can configure DCOM to only use TCP, restrict the ports the client and server use, and open up the firewall just enough to get the communications through. However, the bottom line is these actions seriously compromise the security of your firewall and the communications across it.

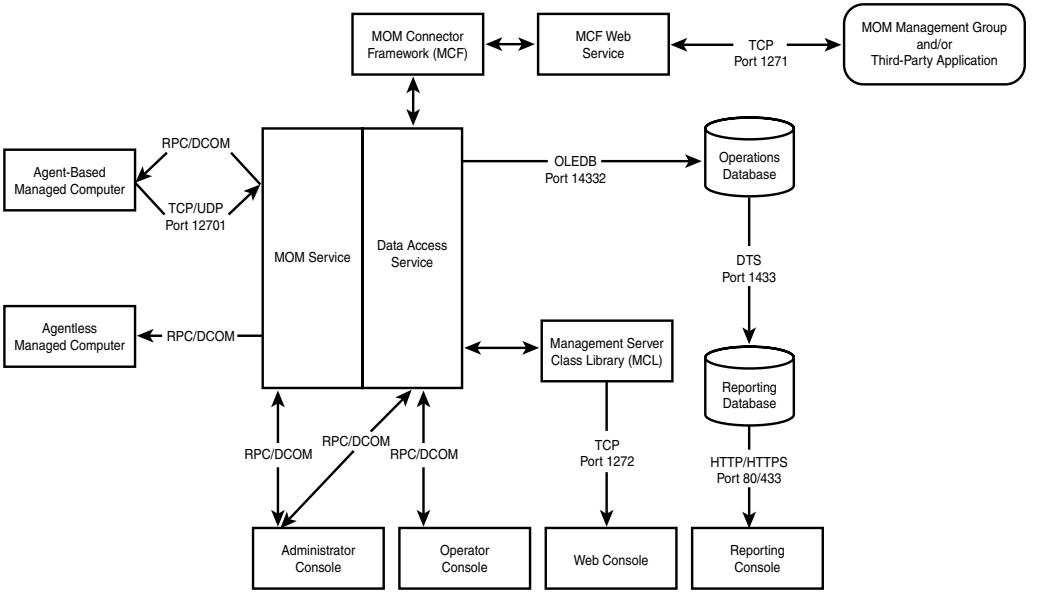


FIGURE 3.4 Component communications protocols and ports.

In keeping with its commitment to the Trustworthy Computing Initiative, Microsoft does not support communications requiring RPC/DCOM across a firewall. Communications are supported which use a standard TCP port that can be secured properly across a firewall, such as the agent-to-management server communications. Table 3.1 lists the various connections, their communications method, and their firewall supportability.

TABLE 3.1 Communications and Firewall Compatibility

From	To	Firewall?	Port, Protocol, or Remark
Agent	Management server	YES	TCP/UDP port 12701
Management server	Agent	NO	RPC (TCP Port 135) and DCOM Ports (TCP/UDP 1024-65535)
Management server	Agentless	NO	RPC (TCP Port 135) and DCOM Ports (TCP/UDP 1024-65535)

TABLE 3.1 Continued

From	To	Firewall?	Port, Protocol, or Remark
Administrator console	Management server	NO	RPC (TCP Port 135) and DCOM Ports (TCP/UDP 1024-65535)
Operator console	Management server	NO	RPC (TCP Port 135) and DCOM Ports (TCP/UDP 1024-65535)
Reporting console	Reporting database	YES	HTTP Port 80 or HTTPS Port 443
Web console	Management server	YES	TCP port 1272
Management server	Operations database	YES	OLEDB Tunneling, port 14332
MOM-to-MOM connector	MOM-to-MOM connector	YES	TCP Port 1271
Connector	Third-party application	YES	TCP Port 1271
Operations database	Reporting database	NO	DTS (TCP Port 1433)

Notice that the agent-to-management server communication method is supported over a firewall, but the management server-to-agent communication method is not. The process of "push" installing agents on managed computers requires RPC and DCOM, whereas the monitoring and rules distribution use a secure TCP port. The downside of this is that if you want to manage an agent on the other side of a firewall, you will have to manually install the agent. Thereafter, the agent will securely initiate the communications. Also, note that managing agentless computers across a firewall is not supported, due to the RPC/DCOM requirements.

The port used by the management server for communicating with agents (12701 by default) is easily configurable on a management server by management server basis. This is also true for the connector port (1271) and the Web console port (1272). You can change the other ports with varying degrees of difficulty.

As Table 3.1 attests, most of the key MOM 2005 communications such as agents and connectors are supported across a firewall, making MOM 2005 a flexible product that can centrally manage your entire enterprise.

How Does MOM Do It?

MOM's internal design and set of components within the management group contains a number of components and complex connections within its architecture. Understanding this architecture can be daunting, so we will approach it by breaking down the layers and looking individually at each component within those layers.

Operations Manager was designed to allow it to deliver all the features in a way that is easy to understand, flexible to a variety of needs, and cost effective. Logically, think of it as being divided into three fundamental layers:

- The data layer
- The business logic layer
- The presentation layer

Organized into logical layers within a management group, MOM provides a high-performance, fault-tolerant, and scalable operations management architecture. These layers, shown in Figure 3.5, each have components working together to deliver the necessary functionality.

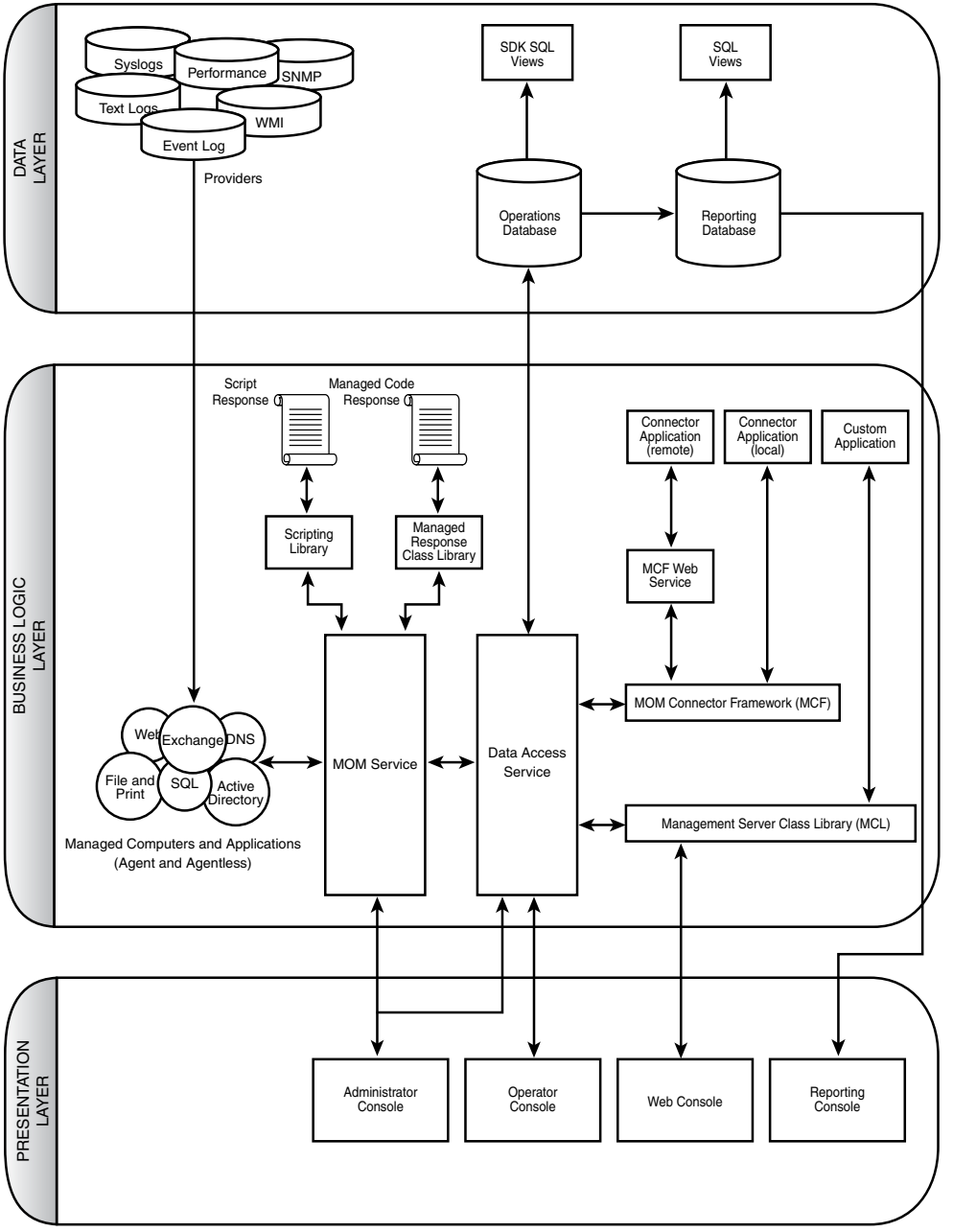


FIGURE 3.5 MOM 2005 architecture and components.

We will look at each of these layers in the following sections of this chapter.

Data Layer

The data layer is the logical layer where the data is stored. This layer is of vital importance to the MOM system, due to the vast quantities of data that need to be received, processed, stored, and acted on. Figure 3.6 shows the data layer and its components.

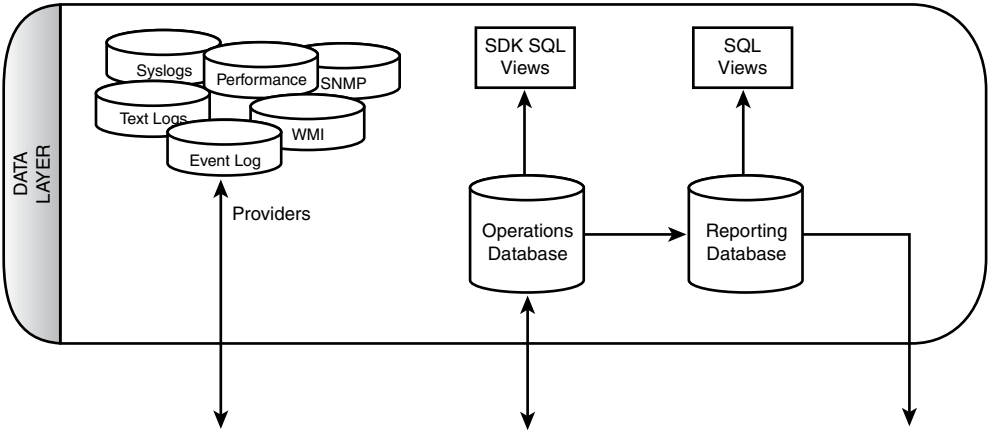


FIGURE 3.6 Data layer and components.

There are five main components within the data layer shown in Figure 3.6:

- Operations database
- Reporting database
- Providers
- SDK SQL views
- SQL views

Without a robust and high-performance data layer, MOM's features would be less effective and could be rendered useless.

Operations Database

The operations database is the centralized repository for MOM's configuration and operational data. This data includes rules, events, performance data, scripts, and the knowledge base. The database engine used is Microsoft SQL 2000 or 2005, either Enterprise or Standard edition. This database is named OnePoint. The name is a holdover from the product's roots before Microsoft acquired MOM and ensures backward compatibility with

MOM 2000. Microsoft plans to change the name of this database in the next version of Operations Manager (see Chapter 23, "Touring Operations Manager 2007," for details).

The OnePoint SQL database is stored in two files by default: the primary database file (EEADATA.MDF) and the transaction log file (EEALOG.LDF), as shown in Figure 3.7. Within the database are more than 350 tables containing the data and configuration settings. Also more than 100 views are defined, providing rapid access to various groupings of the data.

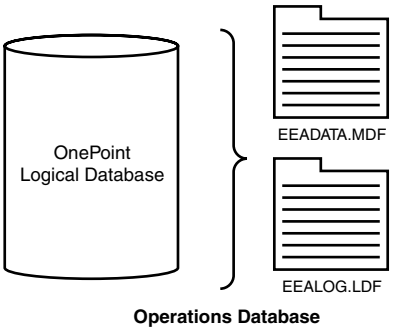


FIGURE 3.7 MOM 2005 database files.

There can be only one operations database in a management group. All collected data, alerts, and configuration data for the management group are stored in the database. This can be a lot of information.

As an example, if the system is collecting data on 100 computers and there are 100 performance counters on each computer measured at 15-minute intervals, there will be close to a million data points collected in a 24-hour period or close to 365 million data points in a year. For 1,000 computers, that would be 3 billion data points per year—and that is just for performance data and does not take into account data from event logs, synthetic transactions, and so on. The sheer quantity of information can be staggering.

The maximum supported size of the MOM 2005 database is 30GB. This limitation is a pragmatic one, in that there is no inherent hard stop limitation built into the MOM code. Exceeding 30GB will not cause the system to halt or fail immediately. The problem is that as the database becomes larger, certain processes such as database grooming take so long to complete that functionality becomes impaired. In the case of database grooming, the database is locked and will not accept additional data while the grooming is taking place. Therefore, management servers collecting data have to buffer the information they have collected and stop accepting new data from agents while the database is locked. Agents then buffer their data while the management server is not accepting data. This can result in delayed alerts because the centralized alerts will not trigger while data is buffered on

the agents. The larger the database, the longer the lockdown window and the more delayed the alerts can get. In a worst-case view, the agent buffers might start overflowing and then information will be lost. Thus, placing an official limit on the database size allows the internal database procedures to complete promptly and the system to function properly.

Real World—Is 30GB Actually a Limitation?

Although 30GB could be considered a limitation, it generally turns out not to be. Our experience with monitoring medium-sized multinational organizations with approximately 250 monitored servers revealed that the operations databases usually held steady within a range of 1.5GB to 2GB. This was using default configuration settings and a standard mix of Microsoft technologies including Windows 2000, Windows Server 2003, Systems Management Server, Exchange 2000 and 2003, and Microsoft SQL Server 2000.

In practice, our conclusion is that the 30GB limit is not going to be a problem for most organizations. Very large organizations monitoring more than 1,000 computers or with heavy monitoring requirements might need to groom more aggressively or increase the number of management groups.

To get around these inherent limitations, MOM includes many features to help maintain the database. Several SQL jobs run automatically to assist in keeping the database trim. The grooming process removes event and performance data that have aged out according to the database grooming setting. Other jobs, created as part of the database installation, perform routine integrity and reindex processes to ensure that the database is healthy and performing well. With the exception of the grooming job, these are standard maintenance jobs that can be performed on any SQL Server database. One job not configured as part of the setup process is the database backup. We discuss procedures for backing up OnePoint and other MOM components in Chapter 12, "Backup and Recovery."

Although the grooming process takes place on a daily basis by default, the actual grooming window is set in the MOM Administrator console under Global Settings. The grooming interval defaults to four days, meaning that events and performance data points older than four days are removed from the operations database when the *MOMx Partitioning and Grooming* job runs at 12:00 a.m. Before the data disappears forever, it is transferred to the reporting database for long-term storage, which we discuss in the next section.

The database is also optimized to allow the grooming to take place quickly, using database partitioning. The database is divided into daily partitions (shown in Figure 3.8). The database is in effect logically broken into daily segments. Grooming and other database-intensive operations can be performed on the logical segments, rather than against the entire database. Most of these operations have specific time constraints, such as grooming data every four days by default or auto-resolving information alerts in four hours. Partitioning allows the database to efficiently retrieve and process the appropriate data.

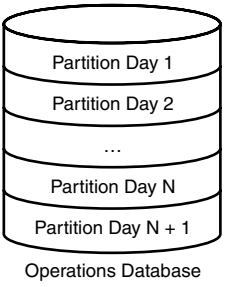


FIGURE 3.8 Operations database partitions.

Reporting Database

The reporting database contains data archived from the operations database. This database is variously referred to as the reporting database, the data warehouse, the archive, and the *System Center Data Warehouse* (SCDW), but the actual SQL Server database name is SystemCenterReporting. The acronym SCDW is frequently used when naming processes within MOM 2005 Reporting, which uses the capacities of the System Center Reporting Server.

As a SQL Server database, the reporting database is stored in two physical files by default: the primary database file (REPDATA.MDF) and the transaction log file (REPLOG.LDF). The database contains more than 100 tables with data and configuration settings. Also more than 300 views are defined, giving the system rapid access to various groupings of the data. These are more views than in the operations database, which makes sense because the reporting database is intended to present information. These views are described in Appendix D, "Database Views."

Data is transferred from the operations database to the reporting database via a Data Transformation Services (DTS) job that runs as a Scheduled Task in the Windows Scheduled Tasks. Similar to the operations database, a job periodically grooms the old data from the reporting database. Both jobs are shown in Table 3.2.

TABLE 3.2 Reporting Jobs

Job Name	Purpose	Default Schedule
SystemCenterDTSPackageTask	Transfers data from the operations database to the reporting database. This job is run as a scheduled task in Windows Scheduled Tasks rather than as an SQL job.	Every day at 1:00 a.m.
SCDWGroomJob	Grooms the SystemCenterReporting database.	Every day at 3:00 a.m.

The grooming interval for the reporting database is one year. The reporting database grooming parameters are hard-coded and buried in a table named WarehouseClassSchema

within the SystemCenterReporting database. The table has a column named WCS_GroomDays that specifies the number of days to groom after, which is 365 for the majority of the data types. The table is keyed on the class ID of the data, so it is not straightforward to modify the information in this table and likely not supported. In the future, Microsoft will provide a user interface method to change these values in a supported manner. Chapter 8, "Post-Installation Tasks," provides information on scheduling the grooming jobs.

Within the one-year grooming window, the reporting database provides a historical view of the operations of your monitored servers. This information is available using reports generated with SQL Server Reporting Services (SSRS).

There is a tentative limit of 200GB for the reporting database, but this is not likely to be the true upper-end boundary. The reporting database growth really only impacts the time needed to generate reports, which does not impact operations functions such as alerting. As the database grows, the database can be separated into different disk subsystems for better performance and even placed on a Storage Area Network (SAN) type technology for performance and growth.

Providers

One of MOM's key advantages is its capability to collect data from a wide variety of sources. This data can be numeric or textual. The information can even reflect missing items that should have occurred within some time frame but did not. This flexibility in the sources of data that MOM can collect and respond to is a key feature in that it allows you to monitor almost anything. For example, many popular brands of Uninterruptible Power Supply (UPS) devices include hardware additions that measure external temperature and humidity. This can be logged to text files or accessed via an Application Program Interface (API). MOM can be configured to read the API or text file, capturing the data and alerting you when the humidity in the server room gets too high or too low.

These sources of data are called *providers*. Provider types include

- **Application logs**—These include the standard event logs, Internet Information Server (IIS) log files, SQL trace log files, ASCII log files, and even UNIX syslog files.
- **Timed events**—These events are generated by MOM and are useful for launching scripts on a regular basis or detecting missing events.
- **Windows Management Instrumentation (WMI) events**—This is a flexible provider, giving MOM access to a wide variety of event-based information through the WMI interface.
- **WMI numeric data**—Similar to the WMI events, this provider gives access to numeric or performance data through the WMI interface.
- **Generic**—This is another class of provider generated by MOM. The Generic provider includes information such as agent heartbeat or events internally generated by scripts.

MOM 2005 includes nearly 700 different predefined providers with its default management packs. You can easily create new providers as needed. Management packs, which are essentially collections of business logic, usually add providers when imported into MOM.

Database Views

MOM includes a number of documented SQL views to help you create custom reports and transfer data from the MOM operations database to other applications and data stores. These views provide read-only access to the MOM database. If you need both read and write access, you can utilize the MOM Windows Management Instrumentation (WMI) classes or the MOM Managed code Application Programming Interface (API), both of which are documented in the MOM Software Development Kit (SDK). The SDK can be accessed at http://go.microsoft.com/fwlink/?LinkId=50272.

The SDK SQL views for the operations database and SQL views to access reporting detail are documented in Appendix D.

Business Logic Layer

The real intelligence of MOM lies in the business logic layer and includes a number of components. Within this layer, rules are set that govern what the business wants to monitor, to be alerted to, to report on, and other myriad details. The business logic layer (shown in Figure 3.9) is where the knowledge of how platforms such as Windows Server 2003 and applications such as Exchange 2003 should be configured and operate are integrated into MOM's framework.

The business logic layer is the most complicated and has the most components of all the layers. The components of this layer are organized into three major groups:

- Core functionality
- Complex responses
- Connecting to external systems

Collecting information from a wide variety of sources is a key characteristic of MOM. This handling of information includes storing it, correlating it to other information, and using it to form alerts and other actions. MOM 2005 collects, handles, analyzes, and responds to operational information using the following components:

- Managed computers and applications
- MOM Service
- Data Access Service (DAS)

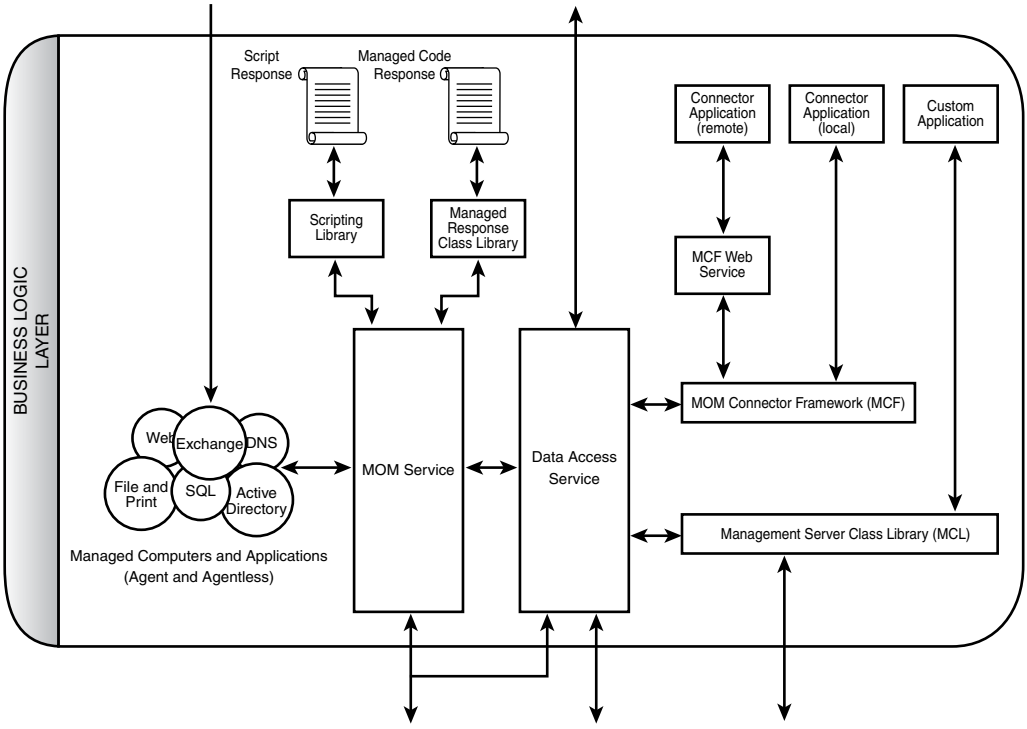


FIGURE 3.9 Business logic layer and components.

The business logic behind a response or task is often more complex or nuanced than even a sophisticated user interface such as MOM's can facilitate. Those cases make it critical that the management application provides a mechanism allowing complex scripts or programs to execute the appropriate business logic. This is accomplished programmatically using the following scripting components:

- Scripting library
- Script responses
- Managed response class library
- Managed code responses

Additionally, the capability to connect to external systems and expose the functionality of MOM 2005 is important to the enterprise scalability and interoperability of MOM. Most large organizations have other management systems or trouble-ticketing systems that are vital to the organizations' operations, and MOM 2005 can interoperate with them. The following components deliver this functionality:

- MOM Connector Framework (MCF)
- Connector applications (local)
- MOM Web Service
- Connector applications (remote)
- Management Service Class Library (MCL)
- Custom applications

We will cover each of the components that make up the functionality of the business logic layer in the next sections. Chapter 19, "Interoperability," discusses the implementation of many of these components.

Managed Computers and Applications—Agent-Based

The method MOM uses for delivering and executing business logic is critical to its success. MOM's agent-based technology allows it to push the work of executing the business logic down to the managed servers. Intelligent local agents are one of the keys to MOM's success. These local agents operate independently, allowing them to respond quickly to changing conditions. The agents are functional even if they cannot contact their management server due to a network outage.

MOM typically manages systems using an installed agent on those systems, although MOM 2005 also includes the capability for agentless monitoring of a small number of systems. The agent runs as a service named the *MOM Service* and collects information as directed by the business logic. The agent is in effect the foot soldier of the MOM system, following the orders dictated by the business logic. The collected information is stored in a buffer locally on the monitored system and then forwarded to a management server. Forwarded information is compressed and encrypted to reduce the footprint on the network and to ensure confidentiality of the management data, allowing MOM to work across slow links and within insecure environments.

Agents can also be configured to look for more than one management server for redundancy and separation of data. Agents can report to a maximum of four management servers, the first of which is assigned automatically by the management service doing the agent install. The other management servers are listed in the agent configuration for automatic fault tolerance. You can see this represented in Figure 3.10, where the agent has a solid line to its primary management server (Monarch) and a dotted line to the other management server (Keystone). The database server is running on a server named Fountain, and the reporting server is Silverthorne.

Normally, the agents are distributed between management servers to provide load balancing as well. This is indicated in Figure 3.11, where Agent 1 reports to Monarch as its primary with Keystone as the backup. However, Agent 2 reports to Keystone as its primary with Monarch as the backup. This balances the management load across the management servers.

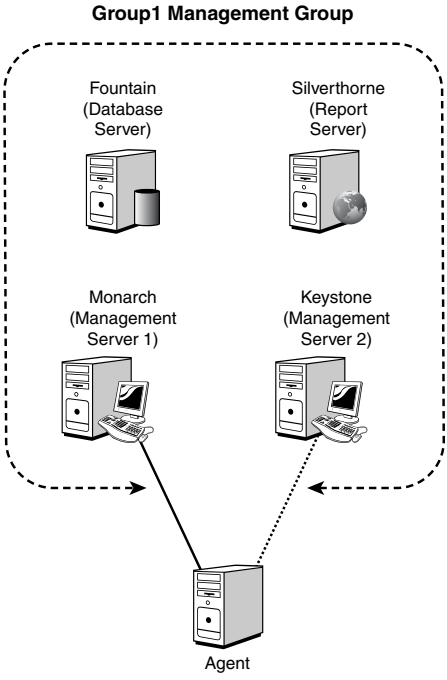


FIGURE 3.10 Agent fault tolerance within a management group.

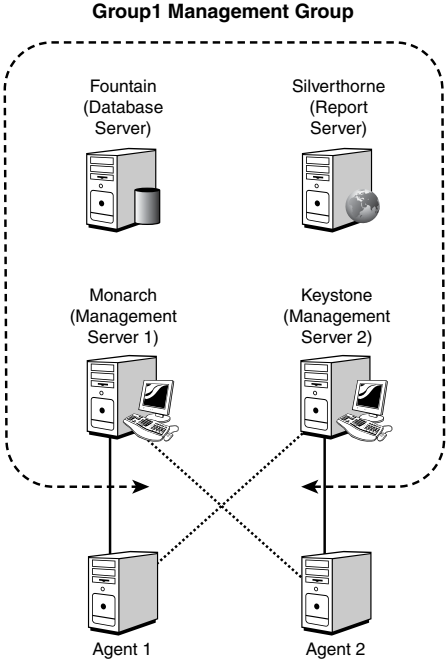


FIGURE 3.11 Agent load balancing within a management group.

Agents can report to multiple management groups as well, which might have different rule sets. This is illustrated in Figure 3.12, where the agent is reporting to both Group1 and Group2. In both management groups, the Monarch management server is primary, and the other management server provides fault tolerance. When reporting to two or more management groups, the agent knows which rules were deployed by which management group and sends the information collected to the appropriate management server. These agents are known as *multihomed*. Chapter 9, "Installing and Configuring Agents," discusses the installation and configuration of agents, including multihomed agents.

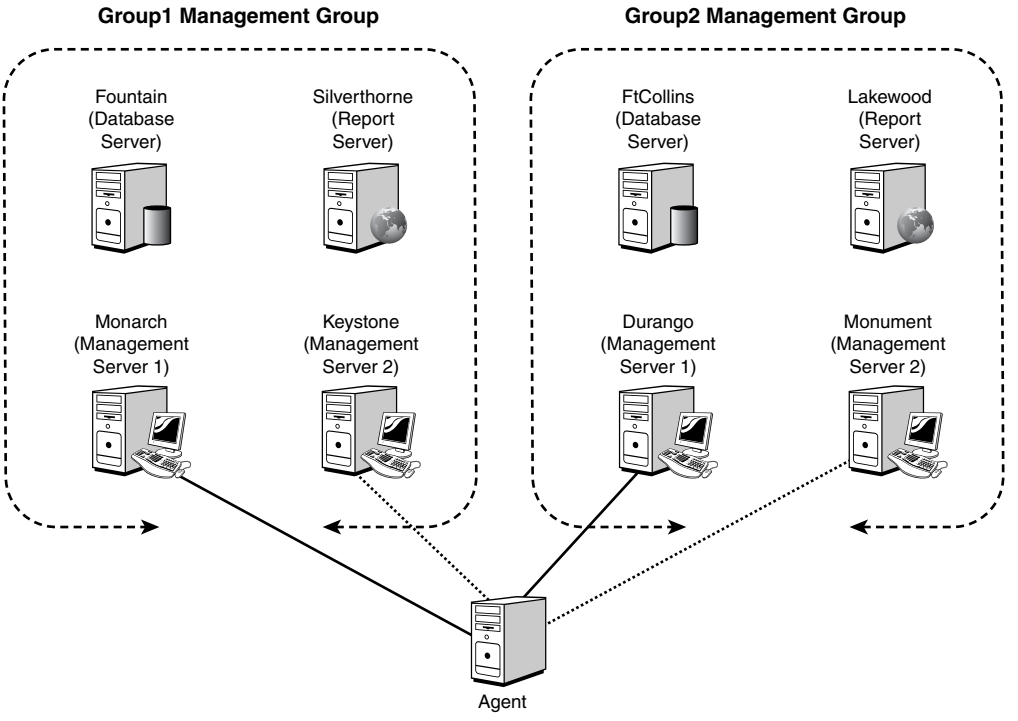


FIGURE 3.12 Agent reporting to multiple management groups.

The agent does not just store and forward the information it gathers to the management groups it reports to. If the business logic dictates, the agent can also evaluate and respond to the information. The responses can be generating an alert, running a script, sending a Simple Network Management Protocol (SNMP) trap, and so on. Having the agents respond locally to events ensures that the system will continue to be monitored and respond to events even when it cannot reach the rest of the MOM infrastructure.

Agents periodically heartbeat to their configured management server. The heartbeat information is used to ascertain whether the agent is still alive and save the management server from having to poll for the status of all its agents. The heartbeat information also contains the latest agent configuration version information. Right after a heartbeat, the

agent also uploads any queued data to the management server. The management server then uses the configuration version information to send the latest configuration information to the agent, ensuring that the agent has the latest business logic applied to it. More information on agent heartbeats is available in Appendix A.

Agent Processes—MOM Service and MOM Host

Although we have been referring to *the agent*, things are actually a bit more complicated than that. The MOM agent actually uses two processes to achieve its objectives: the MOM Service and MOM Host processes, shown in Table 3.3. The MOM Service process handles the internal workings of the agent and communications with the management servers. The MOM Host process handles the information gathering and responses that the business logic dictates. There may be multiple instances of the MOM Host process on any given managed computer. The agent runs multiple MOM Host processes to ensure that the response and providers are isolated. If the process locks running a script or retrieving data from a provider, it will not affect the function of the overall agent or the function of any other MOM Host process.

TABLE 3.3 MOM Agent Processes and Tasks

Processes	Executable	Tasks
MOM Service	MOMService.exe	Communication with management server(s)
		Applications event log—Read/Write
		Security event log—Read/Write
		WMI event provider—Read
		File transfer—Send/Receive
MOM Host	MOMHost.exe	Monitors and collects Windows event log data
		Monitors and collects Windows performance counter data
		Monitors and collects WMI data
		Monitors and collects Application log data
		Runs script and batch responses
		Runs managed code responses

Even with gathering all this information and taking the appropriate actions, the footprint on the monitored system is light. On a typical managed system, agent activities consume less than 1% of processor time. The memory requirements will vary according to number of business logic rules applied to the system, but a rough estimate is between 20 and 60 megabytes. Even the agent on the management servers, where the agent service is handling events from a number of systems, uses less than 1% processor time as an average. Depending on the number of systems managed by a particular management server, the processing time scales with the number of events forwarded and can grow to 5% to 10% of processor time.

MOM can actually tell us what the overhead is. In Figure 3.13, you can see the results for a typical MOM installation monitoring approximately 20 systems. For clarity and simplicity, we selected only three systems for graphing. The graph measures the percentage processor time over the last seven days for the MOM Service process on three systems, including the management server (Monarch). What might not jump out at you is that the scale of the graph is 0% to 1% (the axis values scale automatically based on the values generated). You can see that for most servers the time is less than one-tenth of a percent (.1%). It is interesting to note that in the graph you can see that each of the managed computers has a consistent load, which is proportional to what is being monitored on the server. The exception is the management server itself, which is hovering around 0.25% with spikes of up to about 0.75%. The spike represents the extra work MOM does every day at 2:00 AM to look for new computers. There are also several spikes on 7/12/2006 at about 11 AM and 8 PM, which could bear some investigation. However, even during the spikes the management server load is less than 1% of average processor utilization.

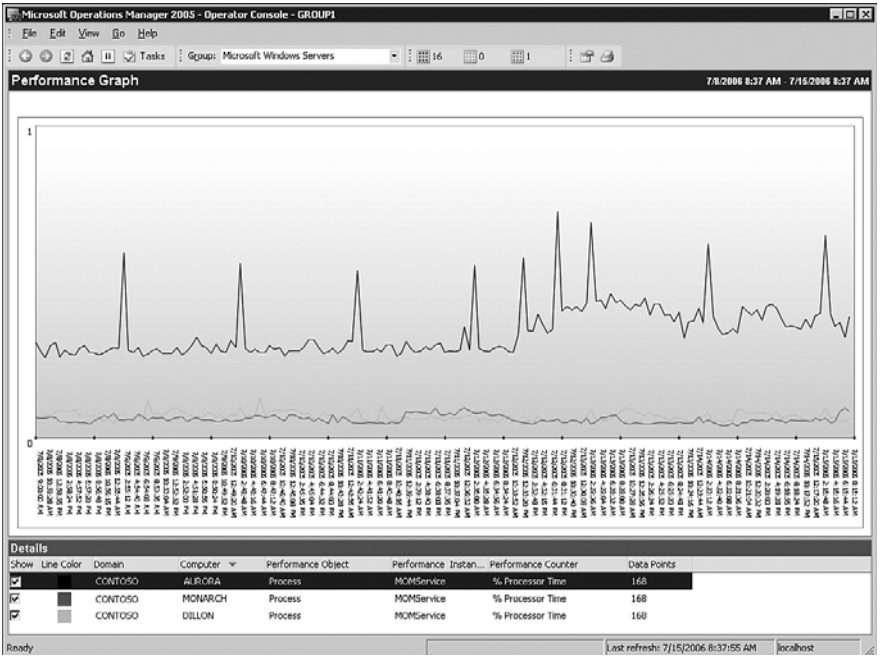


FIGURE 3.13 Typical MOM Service processor utilization.

MOM Service

The memory requirements of the MOM Service process are much more variable, being proportional to what is monitored or the number of rules deployed to the managed computer. Figure 3.14 shows the results of the agent memory utilization over a seven-day period. The roles of the servers are definitely relevant here. The Monarch computer is the MOM 2005 management server, Dillon is a computer running mainly IIS and

antivirus/antispam software, and the Aurora server is running Exchange 2003. The agent on Dillon monitors relatively basic and static functions, so the memory utilization holds steady over the entire seven days at a bit above 6.6 million bytes or about 7MB. The agent on Aurora shows even less variability in the memory utilization but uses more memory and hovers just at under 20MB. This is an Exchange 2003 server and is one of the more managed roles within MOM 2005, hence the higher memory requirements. The agent on Monarch does a variety of other tasks that we will cover in the next section ("MOM Host"), so the memory utilization is much higher and grows from 59MB to just under 66MB.

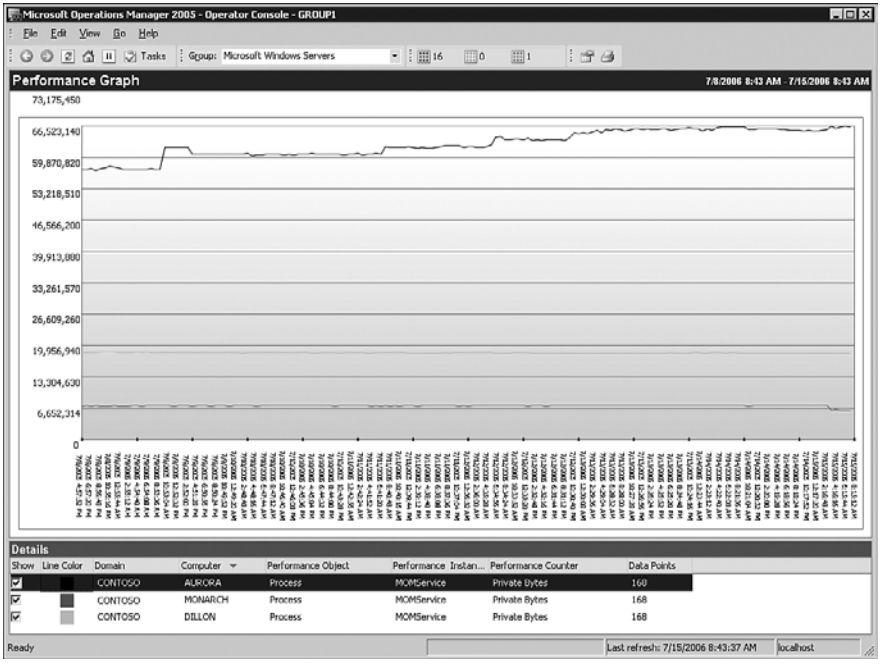


FIGURE 3.14 Typical MOM Service memory utilization.

MOM Host

The other process, the MOM Host, has its own processor and memory utilization patterns. Its processor and memory requirements are separate and in addition to those of the MOM Service process. In Figure 3.15 you can see the processor utilization for the MOM Host processes on the same three computers. The first thing to notice is that there are two instances of the process (MOMHost, MOMHost#1) for each managed computer and in fact there could be more in some cases depending on the different responses and providers that the agent is monitoring. However, you can see that over the course of the seven days of monitoring the requirements for the servers are quite light. For all the servers, the MOMHost instance is close to zero processor utilization, and the MOMHost#1 instance is less than 0.25%. This holds true even for the management server itself.

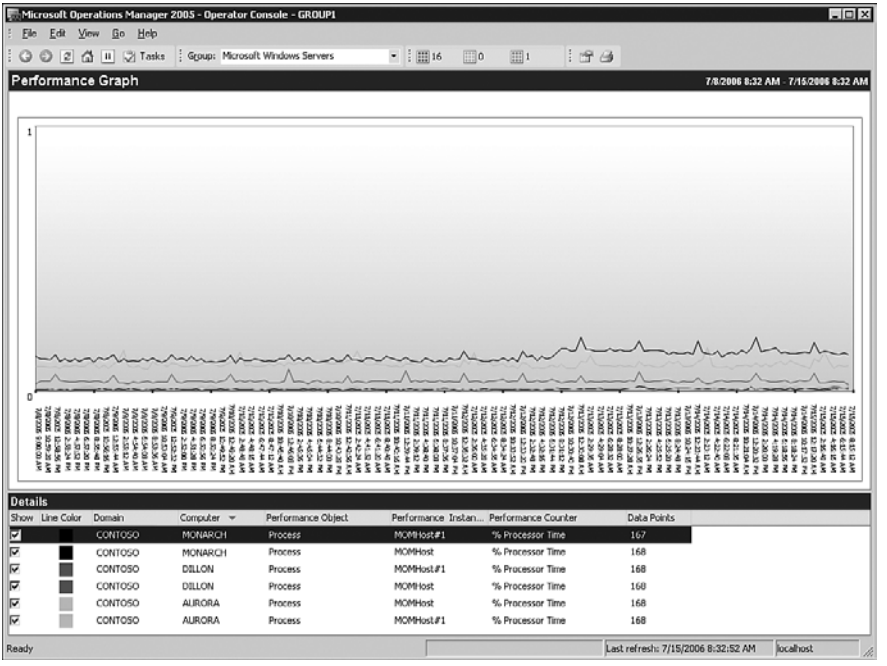


FIGURE 3.15 Typical MOM Host processor utilization.

MOM Host memory utilization tends to be more activity driven than the processor utilization and so exhibits a bit more variability, at least for the second instance of the process (MOMHost#1). The memory requirements again vary by the class of the server and thus by the monitoring requirements. In the case of MOM Host, this is more directly proportional to the level of monitoring. As expected by this, you can see in Figure 3.16 that for the Aurora Exchange server the first instance, the MOMHost process holds steady at just under 10.6MB (or about 11MB), and that the second instance (MOMHost#1) is at just under 21MB at the end of the monitoring period. For the Dillon managed computer, the MOMHost instance is steady at about 7MB, and the MOMHost#1 instance varies between 4MB and 5MB. Finally, the Monarch management server MOMHost instance is steady with a jump midway in the monitoring period at about 8MB, and the second instance, MOMHost#1, hovers right at about 11MB (though there is a brief drop in the middle of the monitoring period). That jump in MOMHost reflects the addition of an agentless managed computer to the management server, which we will discuss in the next section of this chapter.

With all that detailed information, a good question to ask is how much processor and memory resources will be utilized by the agent process overall? As was shown in the previous discussion, it varies by the level of monitoring and the class of server. Our sample computers fall into the categories of a lightly monitored web server, a heavily monitored Exchange server, and a management server. Tables 3.4 and 3.5 show the total processor and memory utilization for the various agent processes in this typical environment.

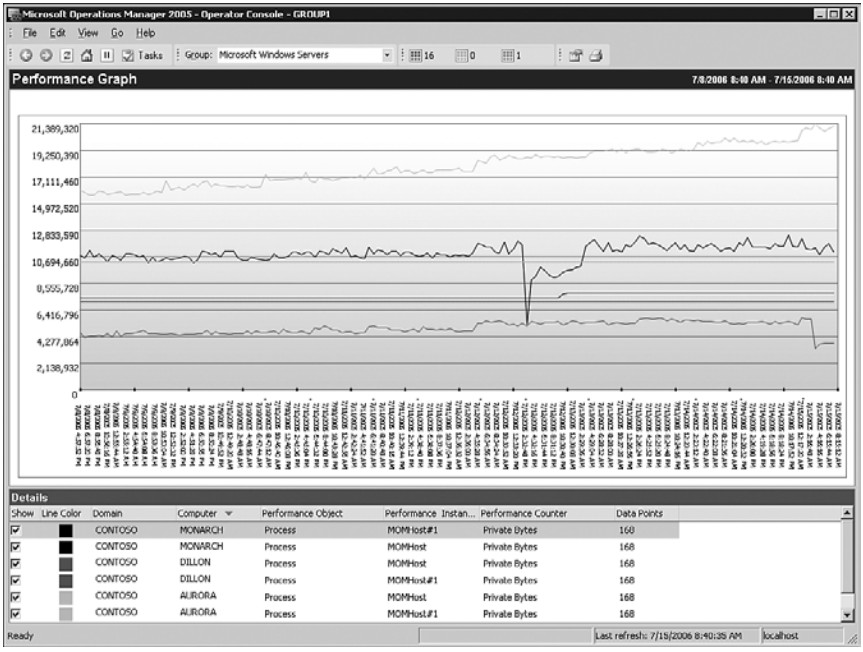


FIGURE 3.16 Typical MOM Host memory utilization.

TABLE 3.4 Typical Agent Memory Utilization

Class	Computer	MOMService	MOMHost	MOMHost#1	Total Memory
Web Server	DILLON	7MB	7MB	5MB	19MB
Exchange Server	AURORA	20MB	11MB	21MB	52MB
Management Server	MONARCH	66MB	8MB	11MB	85MB

TABLE 3.5 Typical Agent Processor Utilization

Class	Computer	MOMService	MOMHost	MOMHost#1	Total Processor
Web Server	DILLON	0.10%	0%	0.25%	0.35%
Exchange Server	AURORA	0.10%	0%	0.25%	0.35%
Management Server	MONARCH	0.75%	0%	0.25%	1.00%

These numbers are not significant, given current memory standards for servers. Even for a web server with only 256MB of RAM, the total agent memory utilization of about 19MB is about 7% of total memory. For a typical Exchange server with 1GB of RAM, the 52MB memory utilization is about 5% of total memory. Even for a typical management server with 1GB of RAM, the 85MB memory utilization is less than 8% of total memory. Far more is used by the SQL Server service! The processor numbers speak for themselves. Table 3.6 summarizes the typical resource utilization on managed computers and management servers.

TABLE 3.6 Typical Utilization Summary

Class	Memory Profile	Processor Utilization	Memory Utilization
Web Server	256MB	0.35%	7%
Exchange Server	1GB	0.35%	5%
Management Server	1GB	1.00%	8%

Managed Computers and Applications—Agentless

In addition to the primary method of managing computers using agent-based technology, MOM 2005 is capable of managing computers without an agent. In this mode, the management server agent takes on the role of the agent for the agentless managed computer. The information is gathered remotely using RPC and DCOM.

The information gathered is equivalent to that for agent-based managed computers. However, agentless monitoring has the following limitations:

- **Scalability**—The work of monitoring agentless managed computers is done by their management server and more specifically by the agent on the management server. This load is significant and can severely impact the performance of the management server, so the agentless mode is limited to only 10 agentless managed computers per management server and a total of 60 agentless managed computers per management group. This is a major limitation to the scalability of the agentless mode of operation.
- **Tasks**—With no local agent on the managed computer, tasks cannot be executed locally on the managed computer. Tasks that run on the management server can be executed against the agentless managed computer, such as the Ping task.
- **Event log descriptions**—Event descriptions are not gathered as part of the agentless monitoring, so the event log descriptions are not available unless the management server has the same event log messages .DLL file. An awkward workaround is to install the same software on the management server as is on the agentless managed computer.
- **Firewall support**—Given that the management server uses RPC and DCOM to monitor the agentless managed computer, agentless managed computers are not supported across a firewall. Opening up RPC and DCOM across a firewall cannot really be done securely, given the nature of the protocols.
- **Management pack limitations**—Management packs presuppose agent-based managed computers and may not fully operate on agentless managed computers. Most of the monitoring functions will work without any problems, but many of the more sophisticated responses will not function correctly.

Given these limitations, the agentless monitoring features are not suitable for many tasks, and this is definitely not the method to manage the majority of computers. However, in some cases such as those where there is concern about the installation of software on an

application server, this will be a solution allowing a reasonable level of monitoring with a limited level of impact to the managed computer. It helps capture those one-off computers that normally resist management.

Agentless Monitoring for Windows NT4 Systems

One use for agentless monitoring is to monitor Windows NT4 systems, as the MOM 2005 agent is not supported on Windows NT4.

MOM Service Component

The MOM Service component (also known as the MOM Server component) is different from the MOM management server. The MOM Service is a component of a management server that runs as a set of services and handles key functionality, which we discuss in this section. The MOM management server refers to a role within the MOM 2005 infrastructure where there are a collection of components on a given computer, including the MOM Service, the DAS, and so on.

The MOM Service performs the following functions for the management server:

- Manages agent installation
- Manages agent configuration
- Monitors managed computer availability
- Consolidates data
- Monitors server-side responses
- Self monitoring
- Monitors agentless managed computers

Using computer discovery rules, the MOM Service component scans the directory for computers that match the computer discovery rules. After discovering computers, the MOM Service component can initiate an agent install and update for the soon-to-be-managed computers. This installation can be configured to take place automatically, or it can require administrative authorization before proceeding. The default is for the system to require approval for agent installations and to wait for 48 hours before removing agents from a system that falls out of the managed computer rules.

In addition, the managed computer attributes are scanned to discover what applications are installed on a managed computer and what roles they play. The attribute scan process is done via a task, which is executed by the agent rather than remotely by the management server. However, the MOM Service component initiates that task and receives the results back from the agents.

Attribute information is used to assign the computer to computer groups within MOM. The MOM Service component is also responsible for scanning computer group

memberships. Membership in computer groups is based on attributes the agent discovers, as well as explicit assignments made at the console. Additional information on computer attributes and group membership formulas is available in Chapter 13, "Administering Management Packs."

Automatic rule deployment and view selection take place after the computer is placed in the appropriate computer groups. Based on the computer group membership, the MOM Service component delivers the appropriate rules to the agents on the managed computers. In this regard, it is the sergeant of a MOM system, passing on the orders for the agents to follow. It is also natural for the business logic and thus the rules that represent that logic to change. These rule updates are automatically distributed to the appropriate managed computers by the MOM Service component.

The agents periodically check in, or heartbeat, to their management server. The MOM Service component receives that heartbeat and also detects when a managed computer has not generated a heartbeat. It is during this heartbeat process that agents check to see whether there are new rules or rule updates that they need to receive from the MOM Service component.

The MOM Service component receives operational data from the agents and passes it on to the DAS component, in effect operating as a proxy between managed computers and DAS. The MOM Service component not only proxies the operational data but also processes the operational data and executes responses indicated by the business logic.

The MOM Service component also performs the agent functions for the management server that it runs on, so you will not find a separate service for the agent on a management server. Finally, the MOM Service component acts as the agent for agentless managed computers. This includes polling of agentless managed computers, collecting the operational data remotely, and running responses (where possible).

Processes Used by the MOM Service Component

Similar to the agent on a managed computer, the MOM Service component uses two processes to achieve its objectives: the MOM Service process and the MOM Host process. The nomenclature is somewhat confusing because there is a *MOM Service component* and a *MOM Service process*. The MOM Service component is composed of two processes, one of which is the MOM Service process. See Figure 3.17 for a graphical view of this.

The tasks, shown in Table 3.7, differ somewhat from agent tasks. The MOM Service process handles the internal workings of the local agent, communications with the agents, and passing the collected information to the DAS component. It also processes the rule updates sent to the agents. The MOM Host processes handle the information gathering and the responses that the business logic dictates for the local computer and for the agentless managed computers. MOM Host also handles the agent installs and uninstalls and updates the configuration settings on the agents.

TABLE 3.7 MOM Service Component Processes and Tasks on the Management Server

Processes	Executable	Tasks
MOM Service	MOMService.exe	Communicates with agents (receiving data and updating rules)
		Relay agent data and rules to and from the DAS component
		Applications event log—Read/Write
		Security event log—Read/Write
		WMI event provider—Read
		File transfer—Send/Receive
MOM Host	MOMHost.exe	Installs and uninstalls agents on managed computers
		Updates agent configuration
		Monitors and collects Windows event log data (local and agentless)
		Monitors and collects Windows performance counter data (local and agentless)
		Monitors and collects WMI data (local and agentless)
		Monitors and collects application log data (local and agentless)
		Runs script and batch responses (server-side, local, and agentless)
		Runs managed code responses (server-side, local, and agentless)

The MOM Service process handles the bulk of the communications with the agent-based managed computers, initiated by the managed computer agent. In contrast, the MOM Host process manages the majority of the communications with the agentless managed computers, and the communications are fundamentally initiated by the management server. This is shown in Figure 3.17.

Data Access Service Component

The Data Access Service (DAS), also known as the Data Access Server, handles both data insertions and data requests to the MOM database. It handles all insertions to the operations database. It handles most of the requests for data as well. The most important exception to this is the reporting subsystem, which bypasses the DAS and uses DTS to transfer data from the operations database to the reporting database. However, the DTS process only copies the data and does not remove data from the operations database.

The DAS is a server-based Component Object Model Plus (COM+) application hosted by the DLLHOST process. The DAS exposes a set of DCOM objects and communicates that control access to the MOM database. The DCOM interfaces are associated with COM+ roles and provide authentication and authorization of the identities that access the interfaces.

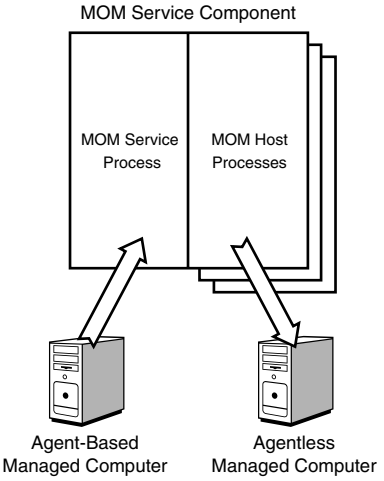


FIGURE 3.17 MOM Service component, processes, and managed computers.

Rather than being installed as a service, the DAS is installed as components in Component Services for improved performance by using object pooling. More than 100 different components are within the DAS. The DAS provides common centralized database access logic, centralized query logic, shared cache, and pooled connections to the operations database server. This translates to improved performance for the database server in reduced connections and duplicate requests, and also for the other components in reduced latency when retrieving cached information. Due to the centralized access and query logic, there is also less likelihood of data being entered incorrectly by wayward components. All components see the same consistent view of the data and operate under a consistent security model.

Some critical services the DAS provides are maintaining data consistency and logging. Whenever a change is made, such as the updating of an alert, the DAS records the change and the credentials of the user making the change, storing it in the operations database as well. This is important for auditing and security.

Programmatic Response Components

The scripting capabilities of MOM 2005 allow for customized monitoring and responses to events, alerts, and performance data.

There are two major types of programmatic responses in MOM 2005:

- **Script responses**—These allow you to extend the capabilities of the basic rules. Scripting responses are flexible and easy to use. MOM supports its own scripting interface with VBScript or JScript, or you can use custom scripting languages such as PerlScript. The scripts are stored within the operations database and are visible and editable from the MOM Administration console.

Another advantage of script responses is that the code and any updates delivered to the managed computer by the management server and agent use the rule delivery process. Scripts can be executed on either the agent or the management server, as appropriate.

- **Managed code responses**—This response type can call a method within a .NET Framework assembly. These assemblies can be developed in any .NET Framework-compliant language such as Visual C# .NET, Visual Basic .NET, Visual C++ .NET, Visual J# .NET, and so on.

  The assemblies are not delivered to the managed computer by the MOM infrastructure, so they require manual distribution and updating.

  A big advantage of the managed code response type is that it can call practically any .NET Framework assembly. These calls can be made either on the managed computer or the management server.

The programmatic responses are supported by two libraries:

- **Scripting library**—The COM-based scripting class library contains various runtime scripting objects, such as the Alert object, Event object, PerfData object, and ScriptContext object. These objects allow response scripts to interact with alerts, events, and performance data. See Chapter 22, "Using and Developing Scripts," for more information.
- **Managed response class library**—The managed code response class library is a .NET Framework class library and is equivalent to the COM-based scripting objects in the scripting library.

  The Microsoft.EnterpriseManagement.Mom.Runtime namespace contains classes and other types for creating MOM-managed code responses. The items in this namespace are defined in the MOM.Context (MOM.Context.dll) assembly.

Table 3.8 compares the capabilities of the two programmatic response types. Overall, script responses are generally easier to use and are better integrated into the MOM 2005 infrastructure. Managed code responses require more effort to create and deploy but perform faster and have a wider array of application interoperability.

TABLE 3.8 Comparison of Programmatic Responses

Feature	Script Responses	Managed Code Responses
Programmatic access to the response context.	Yes	Yes
Capability to create a new alert.	Yes	Yes
Capability to create a new state monitoring alert.	Yes	Yes
Capability to create a new MOM event.	Yes	No

TABLE 3.8 Continued

Feature	Script Responses	Managed Code Responses
Capability to create a new MOM performance data item.	Yes	No
Capability to create and submit computer discovery data.	Yes	No
Supported programming languages.	All COM-compatible scripting languages such as VBScript and JScript, including third-party extensions such as PerlScript	All .NET Framework languages, including third-party extensions
The programming language of the response must be explicitly specified.	Yes	No
Capability to store response as native code.	No	Yes
Stored in MOM database.	Yes	No
Capability to directly invoke an application component from a MOM rule.	No	Yes
Distribution mechanism.	Management Packs	Manual
Deployment mechanism.	MOM agents	Manual
Update mechanism.	MOM agent updates	Manual
Source code can be viewed in the MOM User Interface (UI).	Yes	No
Source code can be edited in the MOM UI.	Yes	No
Capability to call COM components.	Yes (Limited)	Yes
Capability to call .NET assemblies.	Yes (Limited)	Yes

We will look at script responses in more detail in Chapter 22.

Connecting to Other Management Platforms

MOM 2005 is not alone in the enterprise. In a typical enterprise Information Technology (IT) ecosystem, there might be several other management applications ranging from trouble ticket systems to management frameworks. MOM 2005 is designed to integrate with those systems. The integration is fundamentally at the alert level, which supports the following functionality:

- Sending new MOM alerts to external applications
- Sending MOM alert updates to external applications
- Receiving alert updates from external applications to the MOM system
- Receiving new alerts from external applications to the MOM system

In other words, the alert flow is bidirectional. MOM alerts can be forwarded to the other management application and kept in sync on both platforms as the alert changes. Alerts generated in the external management application can be inserted into the MOM database and also kept in sync. For example, if an alert is forwarded to a trouble ticket application, resolving the alert in either the MOM console or the trouble ticket console results in the alert being resolved in both consoles.

In fact, this is the method that MOM 2005 uses to communicate between management groups in a complex MOM hierarchy.

The components that provide the functionality listed previously are

- MOM Connector Framework (MCF)
- MOM Web Service
- Connector applications (local)
- Connector applications (remote)

The MOM Connector Framework is a managed .NET class library that provides an infrastructure for developing connector applications. The MCF manages the communication of alerts and alert updates between MOM 2005 and the connector application. The MCF provides business logic to support the development of custom connectors between MOM and other management applications. The MCF is accessible as both a standalone class library and a web service. Connector applications running locally on the management server can access the class library, and connector applications running remotely need to use the web service. The MCF provides support for connector applications running on non-Windows platforms such as UNIX through the MCF Web Service.

Although similar functionality can be achieved through developing custom applications using the Management Service Class Library (MCL) discussed in the next section of this chapter, there are several advantages to developing connector applications using the MCF. These advantages include the following:

- **Tracking alerts**—The MCF handles the details of tracking which alerts have been forwarded and which ones require updating. This tracking means that the connector application does not need to include the code and logic for those functions, which simplifies the development effort.
- **Crossing firewalls**—The MCF Web service uses port 80 and can easily cross firewalls if needed. The SSL protocol can be used to increase security, in which case port 443 is used, which also crosses firewalls.
- **Alert knowledge**—The MCF also provides easy access to the alert's product knowledge content, if that needs to be forwarded with the alert.
- **Bidirectional logic**—The MCF has built-in logic to handle bidirectional synchronization. The MCF makes it easy to develop two-way connectors, which keep alerts synchronized.

The MCF also allows alert suppression and other logic to be handled using the standard MOM rules. The connector application will not need to perform these tasks, providing better integration into the MOM 2005 infrastructure with less development effort. The rules are stored in management packs and are easily configured by MOM administrators with no need for development skills or controls.

Two namespaces are defined within the MCF. The Microsoft.EnterpriseManagement.Mom.Connector is included for backward compatibility with MOM 2000 SP1. The Microsoft.EnterpriseManagement.Mom.Connector.V2 is the more feature-rich version for MOM 2005 and can also be exposed via a web service on the management server. See the MOM 2005 Software Development Kit (SDK) at http://go.microsoft.com/fwlink/?LinkId=50272 for more information.

Management Service Class Library (MCL) and Custom Applications

The MOM Management Server Class Library (MCL) is used to develop custom applications that access the MOM 2005 operations database programmatically using Visual Studio .NET. The MCL is a .NET Framework class library that exposes MOM operations data, configuration information, and information about the rule hierarchy. This class library is only available on management servers, meaning that the custom applications that use the class library must be developed, tested, and run on the management servers.

The Microsoft.EnterpriseManagement.Mom namespace defines the general-purpose classes and types for accessing MOM operations data, rules, and computers. Items in this namespace are defined in two separate assemblies:

- The Microsoft.Mom.SDK Assembly (in Microsoft.Mom.Sdk.dll)
- The MOM.Context Assembly (in MOM.Context.dll)

Custom applications that use classes in this namespace should reference both assemblies in the Visual Studio .NET project. These assemblies can be found in the SDK Bin folder of the MOM program files folder and in the management server's Global Assembly Cache.

For more information on the Management Server Class Library and its usage, see the MOM 2005 Software Development Kit (SDK), available at the link referenced previously.

Presentation Layer

The last layer of the Microsoft Operations Manager 2005 system is the presentation layer (shown in Figure 3.18), which allows the information gathered by MOM to be viewed and the system to be controlled.

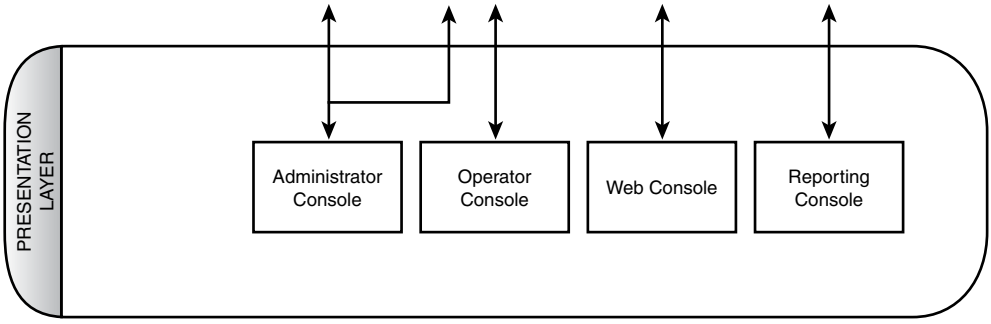


FIGURE 3.18 Presentation layer and components.

Four console components and a reporting subsystem component present the data and provide administrative and operational control of the MOM 2005 system. The consoles are as follows:

- Operator console
- Web console
- Administrator console
- Reporting console

The first two consoles (Operator and Web consoles) support the operations functions for MOM users. These consoles target the operators or IT administrators who actually manage systems and applications. The Administrator console contains the tools used to configure MOM 2005 and is targeted at the MOM administrator. The Reporting console provides access to operational information, both at a detailed operational level and at the broader managerial level. This console is targeted at a range of users from operators to managers and even to executives.

The presentation layer is arguably the most important layer because it is the layer that users of the system interface with. Without a solid presentation layer, the system cannot be used to its maximum potential.

Operator Console

The Operator console presents the operational view of the infrastructure and applications. This is the console in which the most time will be spent by the operators (that is, most users) of MOM 2005, hence the name of the console. This console is roughly modeled on the same lines as the Microsoft Outlook user interface, utilizing the research that Microsoft has invested in developing user interfaces to allow users to view information and complete tasks. It is designed to allow an operator to quickly and successfully handle operational events by doing the following:

- **Identifying**—Knowing that an event has occurred is half the battle in IT. The Operator console rapidly identifies and presents the relevant events and information. It also prioritizes them automatically.
- **Understanding**—Just knowing that an event has occurred is not enough for the operator to be successful. Understanding what an event means, both in the context of other events and with detailed knowledge, is the critical next step in the process. The Operator console delivers in-depth understanding to the operator of the context around the event, detailed knowledge about the event itself, and the event and computer history.
- **Resolving**—Finally, the problem that the event represents needs to be resolved. The Operator console puts both the detailed knowledge of possible solutions and the tasks to execute those solutions at the fingertips of the operator. It can even launch those solutions automatically, while informing the operator of actions taken.

The Operator console is organized to support role-based operators, such as SQL Server administrators, Exchange administrators, or enterprise administrators. The roles can be defined by technology, location, or any other logical grouping. The Operator console allows administrators to monitor and troubleshoot the servers and applications under their responsibility.

The MOM 2005 agents gather a wide variety of information about the managed computers, ranging from configuration to events to performance data. The Operator console displays that variety of information through a number of view types, presented in the following list and discussed more fully in Chapter 8:

- Alerts
- State
- Events
- Performance
- Computers and groups
- Diagram
- Views (Public Views and My Views)

These views can be manipulated in a multitude of ways within the Operator console. The console allows the information to easily perform the following functions:

- **Navigation**—Moving through the various views and the individual items such as alerts and events is a key function of the Operator console. The console is organized to allow operators to easily navigate between views and levels of detail, as well as be able to move back in the same way a web browser would.

- **Scoping**—A big problem with any console is managing the large number of computers, events, and alerts. The Operator console simplifies this by allowing you to set the scope to any computer group, which then narrows the scope of everything that is displayed. For example, if an Exchange administrator selects the Microsoft Exchange Installed Computers group in the console, all the administrator will see as he navigates is the information specific to that group. The groups can be defined geographically or functionally, so a group can be created to follow your IT functional groups and thus narrow the scope as well.

  Even though the scope is adjusted, all the information for all the managed computers is still available in the console should the administrator need to broaden the scope. On the flip side, users can be restricted to their functional scope using Console Scope so that they can see only the information relevant to the group of computers they are responsible for.

- **Drill down**—The Operator console provides summarized views of information but allows you to drill down into the details and back out again. For example, you can click on a state icon in the State view to see the state component view, double-click on the state component to drill into the alerts related to that component, and then drill into the events that generated the alert. You can easily jump all the way back out or go back one level by clicking the Back button.

  Given all the information, complex interrelations, and level of detail inherent in the operational data, the drill-down Operator console makes it easy to navigate through the sea of information.

- **Execute tasks**—The Operator console allows you to easily execute context-sensitive tasks no matter where you are in the console. You can launch a task by selecting a node in a Diagram view, an alert in the Alert view, or a computer in the Computer view. The tasks will launch based on the identity of the computer represented in the information. The tasks are self-policing, meaning that an Exchange task will not allow you to execute it against a non-Exchange computer. This helps prevent unexpected consequences.

The Operator console is an application built on the .NET Framework and is not an MMC console, a departure from the normal Microsoft standard. This is in great part due to the complexity of the UI and the need to present the information in a flexible and fast manner.

The console is organized into four panes composed of the Results Pane and three additional panes, which are the Navigation Pane, the Details Pane, and the Task Pane. The panes are shown in Figure 3.19 and discussed in the following list:

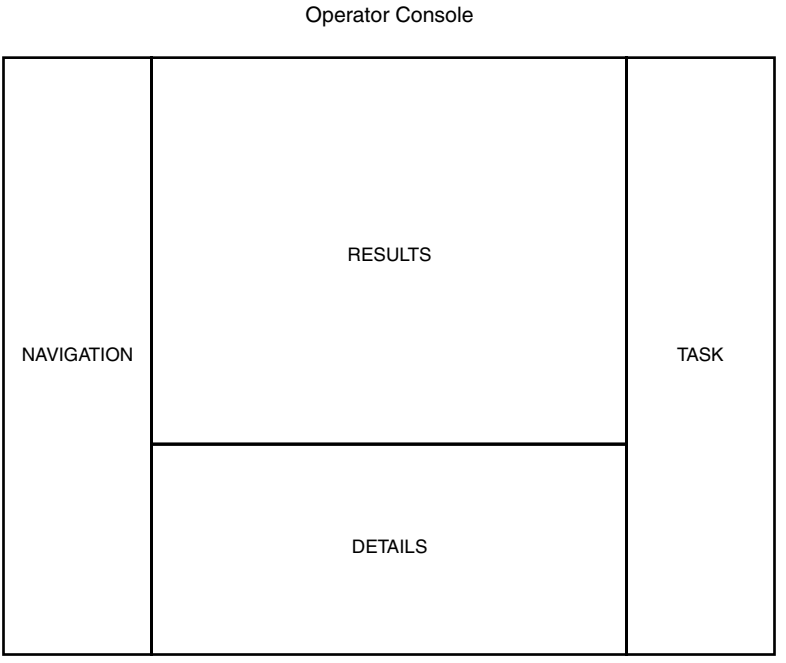


FIGURE 3.19 Operator console organization.

- **Results Pane**—The Results Pane displays the results of a view selection (such as alert or diagram), filtered by the computer group selected. This pane displays the lists of alerts, events, computers, diagrams, and so on—that is, the information that the view is presenting.
- **Navigation Pane**—The Navigation Pane shows a console tree for the currently selected view and the view selection buttons in the bottom of the pane. When a view button is clicked, the console tree adjusts to the appropriate tree, and the active Results Pane changes to reflect the view.
- **Details Pane**—The Details Pane shows the details for the item selected in the Results Pane. There is no Details Pane shown for the Diagram view. The Details Pane is organized by tabs to provide easy access to a wealth of information. For example, the Alert view Details Pane has tabs for Properties, Custom Properties, Events, Product Knowledge, Company Knowledge, and History.
- **Task Pane**—The Task Pane shows a tree view of the tasks and task folders. These tasks are not filtered by context, though they are grayed out if they do not apply to the selected computer.

You can choose not to display the Navigation, Details, and Task panes simply by selecting View within the Operator console and then deselecting the appropriate panes. You can also display up to three different results panes at a time in the Operator console, each

with a different view selected. This is useful if you need to be viewing the state, alerts, and events all at the same time. It is particularly useful if you have a large screen with high resolution!

Web Console

The Web console is a scaled down console that is accessible via HTTP and provides stripped-down versions of the Alerts, Computers, and Events views of the Operator console. It gives computer operators and application owners an easy-to-use and simplified console from which they can check the operational status of their assigned computers or applications. The Web console provides a basic MOM console to a larger group of administrators that manage a narrow set of servers or applications, requiring less training and without installation on their desktops.

As shown in Figure 3.20, you can view alerts, events, and computers, and even change the resolution state of the alert from within the Web console. The console provides full access to any knowledge associated with an alert, which supports the full range of identifying, understanding, and resolving alerts.

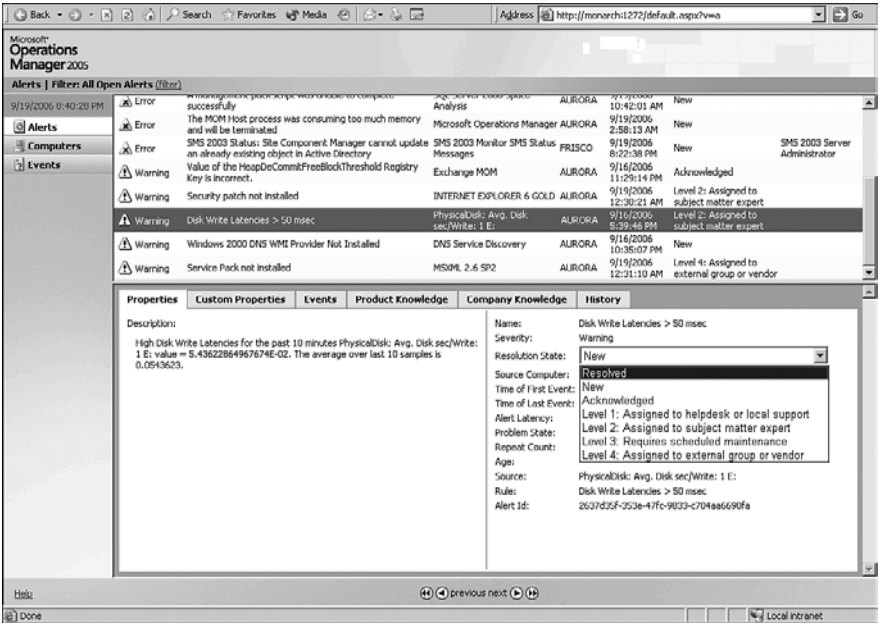


FIGURE 3.20 Web console.

When email notifications are triggered by alerts, the link in the email is a link to the Web console. The default address of the console is http://*<management server name>:1272*. Both the address and the port can be changed within the Administrator console. The Web console can also be launched from within the Administrator console. The default port for the HTTP access is 1272. The port can be changed, and SSL can be used for security.

The Web console is a good example of a custom application that leverages the Management Server Class Libraries (MCL).

Administrator Console

The Administrator console is used to configure and administer MOM 2005 itself. This is the console where the MOM administrators will spend most of their time. In contrast with the Operator console and in keeping with Microsoft standards, the Administrator console is an MMC snap-in.

The console has two panes—the Navigation Pane and the Detail Pane. The Navigation Pane presents a folder type view of the available options. The Detail Pane presents a variety of different types of information and options depending on the particular section being viewed.

The Administrative console is organized into four major segments:

- **Information Center**—The information center provides links to jump to information about MOM 2005, including the MOM 2005 website, downloads, documentation, technical support, licensing, and security. These links allow you to quickly get to the most recent literature and management packs.
- **Operations**—The operations segment presents links to launch the other consoles, including the Operator console, the Reporting console, and the Web console.
- **Management Packs**—This is the segment of the Administrator console where the business logic is maintained. The computer groups, rule groups (or management packs), tasks, notification and operators, scripts, computer attributes, and providers are all accessible from this segment.

  When you click on the Management Packs node in the Navigation Pane, you will see a summary of the business logic in the Detail Pane, as well as links to the other nodes. The business logic summary gives you a count of the rule groups, management pack rules, custom rules, computer groups, and number of scripts.
- **Administration**—The administration segment of the console is the area from which agents are deployed, the mode for managed computers is set, console administration is defined, global settings such as database grooming are defined, and MOM connects to other systems. The sections of the administration segment are Computers, Console Scopes, Global Settings, and Product Connectors.

  When you click on the Administration node in the Navigation Pane, the Detail Pane displays a summary of the MOM 2005 management group architecture and managed computers, as well as links to the other nodes. The management group summary includes the number of management servers, agent-managed computers, agentless managed computers, unmanaged computers, cluster computers, and total number of computers.

What you see in the Navigation Pane of the Administrator console, and the actions that you can take, are determined by your security access. The Administrator console will only display the nodes for the segments in which you have rights. If you have not been granted access to the business logic, the management pack node will not be displayed. If you have not been granted administrative access to the management group, the administration node will not display. MOM security is discussed further in Chapter 11, "Securing MOM."

Reporting Console

The Reporting console is not really a MOM 2005-specific console but rather is the Microsoft SQL Server Reporting Services console. SQL Server Reporting Services is a central and feature-rich solution that enables creating, managing, and delivering both paper-oriented reports and interactive web-based reports from almost any data source, including the SQL Server database. SSRS combines the data management capabilities of SQL Server and Microsoft Windows Server with Microsoft Office components to deliver useful reports.

SSRS supports the full reporting life cycle, including

- **Report authoring**—Report developers can create reports to be published to the Report Server using Microsoft or third-party design tools that use Report Definition Language (RDL), an XML-based industry standard used to define reports.
- **Report management**—Report definitions, folders, and resources are published and managed as a web service. Managed reports can be executed either on demand or on a specified schedule and are cached for consistency and performance.
- **Report delivery**—SSRS supports both on-demand (pull) and event-based (push) delivery of reports. Users can view reports in a web-based format or in email.

The Reporting console allows you to view published MOM 2005 reports, manage security for access to the reports, and manage subscriptions to the reports. Reporting and particularly report creation is a complex topic and will be addressed in detail in Chapter 21, "Using and Developing Reports."

Summary

This chapter introduced the MOM 2005 architecture and data flow. We also discussed components that will be referenced throughout this book. The material in this chapter should help in planning your installation and deployment of MOM. The next chapter discusses the process of planning your MOM deployment.

This page intentionally left blank

PART II

Planning and Installation

IN THIS PART

This page intentionally left blank

CHAPTER 4

Planning Your MOM Deployment

IN THIS CHAPTER

- Assessment
- Design
- Planning
- Proof of Concept
- Pilot
- Implementation
- Maintenance
- Sample Designs

So now that you have had a chance to read about the basics of operations management, what's new in Microsoft Operations Manager (MOM) 2005, and how it works, you are probably ready to start installing—right? Wait just a minute; we need to discuss a major concept before we start deploying or upgrading MOM within your environment: Planning.

Planning your MOM deployment is key to its success. The time spent preparing for your installation is often more important than the time spent actually deploying the product. Most technical product deployments that fail do so because of ineffective planning.

Often in Information Technology (IT) organizations the thought process consists of trying to quickly deploy new products, but this is often done too hastily to actually gain their benefits. We refer to this as the RSA approach: *Ready, Shoot, Aim*. This approach results in technology deployments that are not architected correctly and then require changes, or in some cases complete redeployment to resolve issues identified after deployment is complete. Our recommended approach is RAS: *Ready, Aim, Shoot*.

- Ready—Are you ready to deploy MOM? Assess your environment to better understand it and where MOM 2005 is required.
- Aim—What is the target that you are trying to hit? Based upon your assessment, create a design, and execute both a proof of concept and a pilot project.
- Shoot—Implement the solution that you designed!

The creation of a single high-level planning document is essential because MOM impacts all IT operations throughout the enterprise. Many projects fail due to missed expectations, finger-pointing or the "not invented here" syndrome, which occurs when some IT staff members have vested interests in preexisting or competitive management solutions. These types of problems can be avoided ahead of time by developing a comprehensive plan and getting the backing from the appropriate sponsors within your organization.

A properly planned environment helps answer questions such as the number of MOM management servers you will have, how many management groups to use, the management packs you will deploy, and so forth.

Properly planning for your MOM deployment involves several stages that we will discuss in this chapter: assessment, design, planning, proof of concept, pilot, implementation, and maintenance.

Assessment

The first step in effectively designing and deploying a MOM 2005 solution is to understand the environment. Third-party consultants are typically more than willing to provide assessment documents; organizations can also generate these internally to achieve a similar level of effectiveness. A thorough assessment gathers information from various sources to create a document that is reviewed and updated to ensure that the information it contains is complete and correct.

The principles underlying the importance of assessments are summed up well by Stephen R. Covey's Habit #5, "Seek first to understand, then to be understood," in the *Seven Habits of Highly Effective People* (Simon & Schuster, 1989). In the context of a MOM assessment this means that you should understand the environment before designing a solution. Creating documentation and writing up the nature of your plan are excellent methods to determine whether you understand the topic. This is like studying in school—answering questions builds knowledge much better than just reading the text.

You will want to gather various items for an assessment document:

- Current monitoring solutions—As you assess an environment for a potential MOM 2005 deployment, one of the first tasks is to examine any existing monitoring solutions.

  When evaluating the current monitoring environment, include any server, network, and/or hardware monitoring products in use (including earlier versions of MOM). It is important to understand how these products are being used, what servers or devices they monitor, what servers the monitoring products run on, what operating systems are used on the servers being monitored, who uses them, and how well they are performing. Depending on their functionality and your business's requirements, existing monitoring solutions may be integrated with MOM 2005, replaced by MOM 2005, or not impacted at all by MOM 2005. Understanding the current monitoring environment is an absolutely necessary prerequisite for determining where MOM can integrate into your organization.

- Determine information related specifically to the MOM design itself—As an example, if an earlier version of MOM is currently deployed you most likely will investigate an upgrade deployment (or a side-by-side migration) rather than a new installation of MOM 2005. Chapter 7, "Upgrading to MOM 2005," includes details regarding available deployment options when upgrading MOM. In a manner similar to your assessment of other monitoring products, you will want to determine what MOM is currently monitoring, what functions the servers are providing (such as web applications, directory services, or database servers), and what reporting functionality is required.
- Assess and document current Service Level Agreements (SLAs)—An SLA is a formal written agreement designed to provide the level of support expected—in this case the SLA is from the IT organization to the business itself. For example, the SLA for email servers may be 99.9% uptime during business hours. Some organizations have official SLAs, whereas others have unofficial SLAs.

  An example of an unofficial SLA might be that email cannot go offline during business hours at all. Still other organizations do not have SLAs defined either officially or unofficially. Both types of SLAs should be documented as part of your assessment if you want to take full advantage of MOM 2005's capability to increase server uptime.

MOM and Service Level Agreements

Although MOM 2005's SLA metrics are limited, understanding what SLAs exist in your environment and MOM's role in assisting with those SLAs is an important part of your design.

- Determine the current administrative model for the organization—Organizations are either centralized, decentralized, or a combination of the two. The current administrative model and future plans for the administrative model both help determine where MOM servers may best be located within the organization.
- Existence of help desk or problem management solutions—MOM can be integrated with different types of solutions. For example, connectors are available to connect MOM to Remedy's Action Request System (ARS). There are also connectors for enterprise consoles and management packs for server hardware vendors such as Hewlett Packard and Dell.

  If MOM needs to integrate with any existing solutions, gather details on the name and version of the packages deployed during your assessment phase.
- Service dependencies—Additional assessment and documentation are appropriate for services that MOM may have dependencies on. These include but are not limited to Local Area Network (LAN) / Wide Area Network (WAN) connections and speeds, Domain Name System (DNS), Active Directory, and Exchange. A solid understanding of these services and the ability to document them will improve the design and planning for MOM 2005's deployment.

- Functionality requirements—Assessment is also used in gathering information specific to the functionality required by a MOM 2005 environment. You will want to determine what servers MOM will monitor, what applications on these servers need to be monitored, and how long to retain alerts. It is also important to determine whether reporting will be required for your MOM environment, and if so what specific reports or functionality are required.
- Business and technical requirements—What technical and financial benefits does MOM 2005 need to bring to the organization? The business and technical requirements you gather are critical because they will determine the design you will create. For example, if high server availability is a central requirement, this will significantly impact your MOM 2005 design (which we discuss in Chapter 5, "Planning Complex Configurations"). The business requirements need to be identified, prioritized, and documented; then they can be discussed and revised until agreement on them is achieved.

The information you collect is gathered into a single document called an *assessment document*. This document should be reviewed and discussed by the most appropriate personnel within your organization capable of validating that all the information it contains is correct and comprehensive. These reviews often result, and generally should result, in revisions to the document; it is not to be expected that a centrally written document will get everything right from the get-go. Examine the content of the documents, particularly the business and technical requirements to validate they are correct and properly prioritized. After reaching agreement on the document content, move the project to the next step: designing your MOM solution.

Design

The assessment document you created can now provide the information required to design your MOM environment. In general, it is best to keep the design as simple as possible.

Do not add complexity for the sake of complexity; only when meeting an important business requirement should you go through the effort of adding that element to the design and increasing its complexity. For example, it is best not to create a SQL cluster for MOM reporting functionality unless it is determined that MOM Reporting has a business requirement for high availability. Business requirements are critical because they drive your MOM 2005 design. Rely on your business requirements to determine the correct answer whenever there is a question of how you should be designing your environment.

As an example for what to consider in a MOM 2005 design we will start with the MOM management group.

Management Groups

As a reminder, a management group consists of a MOM database, one or more MOM management servers, MOM consoles (Administrator, Operator, Web, Reporting), and up to

4,000 managed computers. The logical place to start in designing MOM is determining the number and configuration of management groups necessary. Start with one management group and add more if more than one is needed. For most cases, a single management group is the simplest configuration to implement, support, and maintain.

Exceeding Management Group Support Limits

One reason to add an additional management group is if you need to monitor more than the 4,000 managed computers supported in a single management group. The 4,000 managed computers limit is directly impacted by the type of the servers you are monitoring. For example, monitoring many Exchange back-end servers has a far more dramatic impact on a management server's performance than if you were monitoring the same number of Windows XP workstations.

Additionally, if the load on a single server is excessive (the server is reporting excessive MOM queue errors or high CPU, memory, disk, or network utilization), adding another management group can split the load between management groups.

Optimizing the Number of Management Groups

Keep the number of management groups to the smallest number necessary to meet your organization's business requirements.

Separating Administrative Control

Another common reason for establishing multiple management groups is separating control of computer systems between multiple support teams. Let's look at an example where the Application support team is responsible for all application servers, and the Web Technologies team is responsible for all web servers, and each group configures the management packs that apply to the servers that they support.

With a single management group, each group may be configuring the same management packs. In our scenario, the Application support team and Web Technologies team are both responsible for supporting Internet Information Server (IIS) web servers. If these servers are within the same management group, the rules in the management packs are applicable to each of the two support groups. If either team changes the rules within the IIS management pack, it may impact the functionality required by the other team.

In this situation where multiple support groups exist and use the same management packs you will want to implement multiple management groups. In a multiple management group solution, each set of servers has its own management group and can have the rules customized as required for the particular support organization.

Another instance for using multiple management groups would be an organization that has a support group for operating systems and a second support group for applications. Multiple management groups in this scenario allow each group to maintain their own rules, including customizations, without impacting the other support group.

Geographic Locations

Physical location also factors into leveraging multiple MOM management groups. If many servers exist at a single location with localized management personnel, it may be practical to create a management group at that location. Let's look at a situation where a company—Contoso—based in Dallas has 500 servers that will be monitored by MOM; an additional location in Chicago has 250 servers that also will be monitored. Each location has local IT personnel who are responsible for managing their own systems. In this situation separate management groups at each location is a good approach.

Network Environment

If you have a server location with either minimal bandwidth or an unstable network connection, consider adding a management group locally to reduce WAN traffic. Installing a management server at network sites that have between 30 and 100 local systems is typically recommended. MOM 2005 can support up to 50 agent-managed computers on a 128 KB network connection (agent-managed systems use less bandwidth than agentless managed systems).

Multiple Management Group Architectures

Implementing multiple management groups introduces two architectures for management groups—*multitiered* and *multihomed* architectures:

- Multitiered architectures exist when there are multiple management groups with one or more management groups reporting information to another management group.

  As an example with Contoso, it was determined that although Chicago needs autonomy for managing its systems, the Dallas support team needs to have information about the status of the Chicago systems. In this situation, illustrated in Figure 4.1, the Chicago management group can be configured to report its alerts to the Dallas management group to create a multitiered architecture.

How Multitiered Architectures Work

Multitiered architectures are implemented by using the MOM-to-MOM Product Connector (MMPC) on the Source management group and installing the MOM Connector Framework (MCF) on both the Source and Destination management groups. We discuss the MCF and MMPC in Chapter 19, "Interoperability."

- A multihomed architecture exists when a system belongs to multiple management groups, reporting information to each multiple management group.

  For example, Coyote (Contoso's sister company) has a single location based in New York. Coyote also has multiple support teams organized by function. The Operating Systems management team is responsible for monitoring the health of all server operating systems within Coyote, and the Security management team is charged with overseeing the business's security. Each team has its own MOM 2005 management group for monitoring servers. In this scenario a single server running

Windows 2003 with IIS is configured as multihomed and reports information to both the Operating Systems management group and the Security management group.

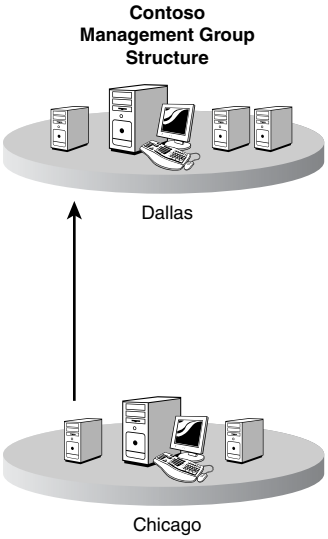


FIGURE 4.1 Multiple management groups.

Another example of where multihoming architectures are useful is when testing or prototyping MOM management groups. With a multihomed architecture, you can continue to report to your production MOM management group while also reporting to a new or testing management group. This allows testing of the new management group without impacting the existing production monitoring.

Limits on Multihomed Systems

A multihomed agent can belong to a maximum of four management groups. The registry contains a separate subkey under HKLM\SOFTWARE\Mission Critical Software\OnePoint\Configurations for each MOM management group that the agent belongs to.

Additional information on registry keys used in MOM 2005 is documented in Appendix B, "Registry Settings."

MOM Servers

The number and location of MOM servers in your environment is directly related to the number of management groups. The server roles in a management group include the

MOM database, MOM management servers, MOM reporting servers, MOM reporting databases and MOM consoles. In a small environment all of these roles can be on a single server with sufficient hardware resources. As with management groups, it is best to keep things simple by keeping the number of MOM servers as low as possible while still meeting your business requirements.

Minimum Hardware Requirements

The general industry standard is that the server you choose should be technologically viable for three to five years following deployment. Buying a less expensive server may save some money in the short term, but when that server needs to be replaced in two years, your costs will be significantly more. We recommend that all MOM servers should satisfy at least the minimal technical requirements listed in Table 4.1.

TABLE 4.1 Server Minimum Hardware Requirements

Hardware	Requirement
Processor	550MHz Pentium
RAM	512MB
Disk	5GB Space
CD-ROM	Needed
Display adapter	Super VGA
Monitor	800x600 Resolution
Mouse	Needed
Network	10Mbps

This is the bare minimum hardware that the software requires to simply function. No IT organization worth its salt would deploy on the minimum hardware specification unless it needed only the minimal functionality. The actual hardware platform you deploy on needs to be larger and scaled based on the capacity requirements of the number of agents you deploy and how the system is configured.

Table 4.2 presents a more realistic minimum server requirement. These reflect the actual processing, memory, and network requirements needed by the MOM components.

TABLE 4.2 Realistic Server Hardware Requirements

Hardware	Requirement
Processor	2.4GHz P4
RAM	1GB
Disk	36GB (varies by component)
CD-ROM	Needed
Display adapter	Super VGA
Monitor	1024x768 Resolution
Mouse	Needed
Network	100Mbps

Keep in mind that if your organization has plans to expand the list of servers to be monitored, your MOM implementation will need to expand its role accordingly. It is therefore wise to keep future expansion in mind when sizing your servers.

Minimum Software Requirements

One of the more obvious software prerequisites for the installation of MOM is a Windows operating system. However, operating system requirements for the components vary somewhat because the various components comprising the MOM infrastructure have different operating system requirements. Table 4.3 and Table 4.4 list the various operating systems and their suitability for MOM components. These tables assume that you have installed the latest service pack of each operating system.

Note that the MOM components are at this time all 32-bit versions and that there are known issues when attempting to run on 64-bit operating systems. All the versions addressed in this chapter are 32-bit unless otherwise noted, with the exception of agent support.

TABLE 4.3 Server Component Operating System Support

Operating System	Management Server	Database Server	Report Server
Microsoft Windows Server 2003, Standard Edition	X	X	X
Microsoft Windows Server 2003, Enterprise Edition	X	X	X
Microsoft Windows Server 2003, Datacenter Edition	X	X	X
Microsoft Windows Server 2003, Web Edition	X	X	X
Microsoft Windows Small Business Server 2003	X	X	X
Microsoft Windows Server 2003 64-bit AMD, Standard Edition	X	X	X
Microsoft Windows Server 2003 64-bit AMD, Enterprise Edition	X	X	X
Microsoft Windows Server 2003 64-bit AMD, Datacenter Edition	X	X	X
Microsoft Windows Server 2003, Web Edition	X	X	X
Microsoft Windows Server 2003 64-bit Itanium, Enterprise Edition		X	
Microsoft Windows Server 2003 64-bit Itanium, Datacenter Edition		X	
Microsoft Windows XP Professional			
Microsoft Windows 2000 Server SP4+	X	X	X
Microsoft Windows 2000 Advanced Server SP4+	X	X	X
Microsoft Windows 2000 Datacenter Server SP4+	X	X	X
Microsoft Windows 2000 Professional SP4+			
Microsoft Windows NT 4.0 Server			
Microsoft Windows NT 4.0 Server Enterprise Edition			
Microsoft Windows NT 4.0 Server Terminal Server Edition			

MOM Database on 64-Bit Operating System

The MOM database will need to be created manually on 64-bit operating systems using the 64-bit version of the :MOMCreatedb.exe tool. This can be found on the installation CD. Contact Microsoft for an updated version of :MOMCreatedb if you are using a 64-bit version of SQL Server 2005 (see http://support.microsoft.com/kb/921278/ for additional information).

Even though the components will run on some 64-bit operating systems, they actually are in 32-bit Windows on Windows (WOW) mode. MOM 2005 does not really benefit from the expanded capabilities offered by the 64-bit operating systems, although it is supported in a 64-bit environment.

TABLE 4.4 Console Operating System Support

Operating System	Administrator Console	Operator Console	Web Console
Microsoft Windows Server 2003, Standard Edition	X	X	X
Microsoft Windows Server 2003, Enterprise Edition	X	X	X
Microsoft Windows Server 2003, Datacenter Edition	X	X	X
Microsoft Windows Server 2003, Web Edition			
Microsoft Windows Small Business Server 2003			
Microsoft Windows Server 2003 64-bit AMD, Standard Edition	X	X	X
Microsoft Windows Server 2003 64-bit AMD, Enterprise Edition	X	X	X
Microsoft Windows Server 2003 64-bit AMD, Datacenter Edition	X	X	X
Microsoft Windows Server 2003, Web Edition	X	X	X
Microsoft Windows Server 2003 64-bit Itanium, Enterprise Edition			
Microsoft Windows Server 2003 64-bit Itanium, Datacenter Edition			
Microsoft Windows XP Professional SP1+	X	X	X
Microsoft Windows XP 64-bit AMD	X	X	X
Microsoft Windows 2000 Server SP4+	X	X	X
Microsoft Windows 2000 Advanced Server SP4+	X	X	X
Microsoft Windows 2000 Datacenter Server SP4+	X	X	X
Microsoft Windows 2000 Professional SP4+	X	X	X
Microsoft Windows NT 4.0 Server			
Microsoft Windows NT 4.0 Server Enterprise Edition			
Microsoft Windows NT 4.0 Server Terminal Server Edition			

Although MOM 2005 supports a variety of operating systems for its components, we recommend using Windows Server 2003 Service Pack 1 (SP1). The MOM components are optimized to run under Windows Server 2003, and SP1 even includes a specific role for MOM 2005.

MOM 2005 requires a database to store the configuration and operations data. Table 4.5 lists the MOM support for the various database versions.

TABLE 4.5 Database Requirements

Database Component	Operations Database	Reporting Database
Microsoft SQL Server 2005	X	X
Microsoft SQL Server 2000	X	X
Microsoft SQL Server 2000 Desktop Engine (MSDE) (MOM 2005 Workgroup Edition Only)	X	

Requirements for Monitored Computers

Managed computers have similar minimum requirements to load the agent (shown in Table 4.6), though they are significantly less stringent than the server requirements.

TABLE 4.6 Managed Computer Requirements

Hardware	Requirement
Processor	200MHz Pentium
RAM	128MB
Disk	100MB

These requirements represent the bare minimum required for the client software to function. It is always recommended to exceed minimum requirements to protect your investment for the long term.

The MOM 2005 platform supports monitoring the current 32-bit and 64-bit operating systems ranging from Windows NT through Windows Server 2003, with the exception of some versions of Windows XP. Table 4.7 lists the operating system requirements for each of the agent modes.

TABLE 4.7 Agent Component Operating System Support

Operating System	Agent (32-bit)	Agent (64-bit)	Agentless
Microsoft Windows Server 2003, Standard Edition	X		X
Microsoft Windows Server 2003, Enterprise Edition	X		X
Microsoft Windows Server 2003, Datacenter Edition	X		X
Microsoft Windows Server 2003, Web Edition	X		X
Microsoft Windows Small Business Server 2003	X		X
Microsoft Windows Server 2003 64-bit AMD, Standard Edition	X		X

TABLE 4.7 Continued

Operating System	Agent (32-bit)	Agent (64-bit)	Agentless
Microsoft Windows Server 2003 64-bit AMD, Enterprise Edition	X		X
Microsoft Windows Server 2003 64-bit AMD, Datacenter Edition	X		X
Microsoft Windows Server 2003, Web Edition	X		X
Microsoft Windows Server 2003 64-bit Itanium, Enterprise Edition		X	X
Microsoft Windows Server 2003 64-bit Itanium, Datacenter Edition		X	X
Microsoft Windows XP Professional SP 1+	X		X
Microsoft Windows XP 64-bit AMD	X		X
Windows XP Home Edition			
Windows XP Media Center Edition			
Windows XP Tablet PC Edition			
Windows XP Embedded			
Microsoft Windows 2000 Server	X		X
Microsoft Windows 2000 Advanced Server	X		X
Microsoft Windows 2000 Datacenter Server	X		X
Microsoft Windows 2000 Professional	X		X
Microsoft Windows NT 4.0 Server SP 6			X
Microsoft Windows NT 4.0 Server Enterprise Edition SP 6			X
Microsoft Windows NT 4.0 Server Terminal Server Edition SP 6			X

In addition to the software minimums, agent installation will not occur if the MOM Action account chosen does not have local administrative rights on the agent computer. If this is not possible, the agent can be manually installed from the Manual Agent Install folder located on the MOM setup CD. However, the account that runs the Manual Agent Setup executable must still have local admin rights on that machine. The default is typically to run the agent under the Local System account. More detail about agents is available in Chapter 9, "Installing and Configuring Agents."

Management Server

The primary function of a management server is providing communication between the monitored servers and the MOM database. The number of management servers required depends on the business requirements identified during the assessment:

- If redundancy is a requirement you will need at least two management servers per management group. Each management server can handle up to 2,000 agent managed computers and up to 10 agentless managed computers.

  If a management group in your organization needs to monitor more than 2,000 computers, multiple management servers should be installed in the management group.

- Each management group must have at least one management server in that management group.

The general specifications for a MOM 2005 management server is a Pentium 4 processor with one gigabyte of memory, with heavier utilized management servers requiring a dual Pentium 4 processor with one gigabyte of memory. (These requirements are based on our experience rather than Microsoft's official hardware recommendations.) Server redundancy is achieved by installing multiple management servers in a management group.

Using a design of 1,000 managed computers for purposes of discussion, there should be multiple management servers. Each management server needs to support one-half the load during normal operation and the full load during failover situations. Table 4.8 shows a standard configuration that could easily support up to 500 managed computers.

TABLE 4.8 Standard Management Server to Support 500 Managed Computers

Hardware	Requirement
Processor	Dual 2.4GHz P4
RAM	1GB
Disk	36GB
CD-ROM	Needed
Display adapter	Super VGA
Monitor	1024x768 Resolution
Mouse	Needed
Network	100Mbps

As you can see, the specification for the management server does not call for a powerful system. The management server is efficient and does not store any appreciable volume of data, relying mostly on processor, memory, and network throughput.

You would want to have four management servers to support fault tolerance and load balancing, each capable of supporting 500 computers. However, you would want to have each configured to support only 250 computers during normal operations so that they would not be overloaded in the case of a failover.

When you design for redundancy, plan for each server to have the capacity to handle not only the agents it is responsible for but also the agents it will be responsible for in a failover situation. For example, with a two management server configuration, if either management server fails, the second needs to have sufficient resources to handle the entire agent load.

Management Server Placement Management servers should be kept separate from the MOM database server in anything but a single server MOM configuration. In a single server configuration one server encompasses all of the MOM roles including the management server and the database server.

Using the Same Server for Management Server and Database Server

If the management server and database server roles are combined on the same server, we recommend monitoring no more than 200 agents on that server because it can degrade performance of your MOM solution. If you will be monitoring more than 200 agents you should split these roles to separate your servers.

Planning for Licensing Part of your decision regarding server placement should include evaluating licensing options for MOM 2005. Microsoft provides a licensing discussion at http://www.microsoft.com/mom/howtobuy/demo/presentation.html. To determine licensing costs, remember that you need to acquire a MOM 2005 license for each MOM server, plus Operations Management Licenses (OMLs) for each device monitored by MOM.

When the database server is placed separately from the management server, the following licensing aspects should be considered:

- If the SQL Server is licensed per processor, no Client Access Licenses (CALs) are required.
- If the SQL Server is licensed per user, CALs are required for each managed device.
- If the SQL Server is licensed using the MOM with the SQL 2005 Technologies license, no CALs are required. The SQL license in this case is restricted to supporting only the MOM database and application—no other databases or applications can use that instance of SQL Server.

For the most current information on MOM 2005 pricing and licensing, refer to Microsoft's website at http://www.microsoft.com/mom/howtobuy/.

Database Server

The MOM database server hosts the MOM 2005 OnePoint database. The MOM database server can run on either a single server or a cluster; a cluster is recommended if your business requirements for MOM include high-availability and redundancy capabilities. Each management group must have a MOM database. The MOM database is critical to the operation of your management group—if it is not running, the entire management group has limited functionality. This is not to say that the agents are not still monitoring issues and sending them to the management server, but if the MOM database is down, the information is not added to the database, consoles do not function, and eventually the queues on the agent and the management server completely fill.

MOM and Queues

By default, the agent has a configurable 3MB queue that is used when communication is lost to the primary/failover Management Server. This queue generally fills in about a day and a half (depending on the amount of data a particular agent sends to the management server) if communication is not reestablished.

The Management Server has a configurable 30MB queue that is used if the link between the management server and the database server is lost.

Additional information on the queues used by MOM is included in Appendix A, "MOM Internals."

Install the MOM 2005 database server on a dual Pentium 4 processor with a minimum of one gigabyte of memory. Heavier utilized servers may need up to a quad Pentium 4 processor with two gigabytes of memory. The more memory you give it, the better SQL Server performs. Redundancy for these servers is provided via clustering using an Active/Passive configuration. The MOM database server can use an Active/Active configuration (MOM 2005 SP1 and above) but this is not our recommended design. Details on using an Active/Active configuration is discussed in Chapter 10, "Complex and High Performance Configurations."

We recommend that you not install the MOM database server with the management server in anything but a single server MOM configuration. Although the database server can coexist with the MOM reporting database server, this may also cause contention for resources, resulting in negative impact on your MOM environment.

Database Server Performance

Database server performance is strongly impacted by its disk configuration. Configuring your MOM database server with the fastest disks available will significantly improve the performance of your management group. We discuss additional information on this topic including recommended RAID configurations in Chapter 10.

Alert latency is the best measure of performance of the MOM system because the time it takes MOM to detect a problem and notify an administrator is a key performance metric. If there is a delay in receiving this information, the problem could go undetected. Due to the criticality of this measure, MOM Service Level Agreements are typically based on alert latency.

Table 4.9 shows database server hardware specifications for supporting up to 1,000 nodes. This table shows the increased performance requirements that 1,000 agents place on processor, memory, and disk space for the database server.

TABLE 4.9 Standard Database Server to Support 1,000 Nodes

Hardware	Requirement
Processor	Quad 2.4GHz P4
RAM	2GB
Disk	OS: RAID1 72GB
	LOG: RAID1 72GB
	DATA: RAID5 200GB
CD-ROM	Needed
Display adapter	Super VGA
Monitor	1024x768 Resolution
Mouse	Needed
Network	100Mbps

For performance purposes, it is better for the database server to have only the MOM database components on it. Remember that the database can only grow to a 30GB supported maximum, so there is a limit on the size the system can be. However, there will be heavy database activity, so having separate channels for the database logs and data is a key optimization.

The rationale for allocating 200GB to a disk with a database that should stay within 30GB is to allow for emergency growth and database operations such as backup.

Real World—Data in the MOM Database

If you monitor 100 servers and store data for four days, the starting point for the MOM database will be at least 2000 megabytes or 2GB. The formula used here to calculate the 2000 megabytes (MB) is database size = (servers * grooming days * 5MB). This number is based on deploying a small number of management packs and should be used only as a rough initial estimate for the MOM database size. In some organizations with a high number of active management packs we have seen systems requiring 75 megabytes of data per day per server (and in one case 120 megabytes of data per day per server with a misconfigured management pack).

If you have more than just a few management packs, this amount would be adjusted by a factor that varies depending on your servers and the number and types of management packs deployed in your environment. Details on how to estimate the size of the MOM database are included in Chapter 10.

Reporting Server

The MOM Reporting server hosts the SystemCenterReporting database MOM 2005 uses for web-based reports. The reporting database typically runs on a single server but can be run on a cluster if high-availability and redundancy are required for MOM Reporting.

The MOM 2005 reporting database server should be at least a dual Pentium 4 processor with one gigabyte of memory. More heavily utilized servers may use up to a quad Pentium 4 processor with two gigabytes of memory. For reasons similar to the requirements for the MOM database, this server should not coexist on the same system hosting the management server.

As mentioned previously in the "Database Server" section of this chapter, the two databases may reside on the same database server, but this can result in contention problems. When both databases exist on the same physical hardware and an intensive web report is run, it can slow down performance of the MOM database server, causing a delay within the consoles and other functions utilizing the MOM database.

Database Sizes

There is a direct relationship between the size of the MOM database and the MOM reporting database. If the MOM operational database is currently storing 10 gigabytes of data for one month of history, the reporting database will start at approximately 13 times this value or a total of gigabytes. The default setting for the MOM reporting database is 395 days of data retention (13 months) to provide the capability to provide a

trending report with history over one year. It is recommended to design your SQL Server using separate disks for logs and data files. Details on best practices for architecting the SQL drive configuration are discussed in Chapter 10.

In support article 887016, Microsoft provides information on changing the number of days data is retained in the SystemCenterReporting database. Another good article related to the OnePoint and SystemCenterReporting database sizes is 899158, which discusses troubleshooting DTS and database sizing issues for the MOM 2005 reporting database. These articles are available on the Microsoft Support website, http://support.microsoft.com.

The reporting server hosts the reporting database and the SQL Server Reporting Services engine used to generate the MOM reports. Table 4.10 shows the reporting server specifications.

TABLE 4.10 Standard Reporting Server to Support 1,000 Nodes

Hardware	Requirement
Processor	Dual 2.4GHz P4
RAM	2GB
Disk	OS: RAID1 72GB
	LOG: RAID1 72GB
	DATA: RAID5 or SAN 2TB
CD-ROM	Needed
Display adapter	Super VGA
Monitor	1024x768 Resolution
Mouse	Needed
Network	100Mbps

The processing requirements for the reporting server are lower than for the (operational) database server, but the storage requirements are similar in configuration and larger in scale. See Table 4.20 later in this chapter, but for 1,000 agents for one year the total reporting server storage would be approximately 2 terabytes (TB). This would have to be managed for supportability, using archive databases or another method.

Web Reporting

MOM 2005's web reporting is an additional component of MOM 2005. The web reporting server interacts with SQL 2000 Reporting Services to display reports in the Reporting console. Typically the web reporting server runs on a single server.

You can add redundancy to web reporting by installing multiple web reporting servers and leveraging Network Load Balancing (NLB) or other load balancing solutions. The MOM 2005 web reporting server should be at least a Pentium 4 processor with one gigabyte of memory; for more heavily used servers you may configure a dual Pentium 4 processor with one gigabyte of memory. Web reporting is often run on the MOM reporting database server when sufficient processing resources are available.

MOM Consoles

The MOM consoles are another component of MOM 2005. The MOM consoles include the Administrator console, Operator console, Web console, and Reporting console. The Web and Reporting consoles are web-based interfaces, and the Administrator console is a standard Microsoft Management Console (MMC). The Operator console and Administrator console should be installed on the management server and can also be installed on desktop systems running Windows XP. Installing these consoles on another system removes some of the load from the management server. Desktop access to the consoles also simplifies administration.

Installing Consoles

By default, the MOM installation process installs the Operator and Administrator consoles on the management server. For ease in administration, you can also install them separately on administrator and operator consoles in your environment.

The number of consoles a management group supports is also an important design specification. The reason is that as the number of consoles active in a management group grows, the database load also grows. This accelerates as the number of managed computers increases. This is because consoles, either operator or web-based, increase the number of database queries.

The net effect is that each additional console adds roughly a 3% load on the database server, assuming a standard 1 minute refresh rate for each console and 1,000 managed computers. The processor utilization of the database server grows linearly with the addition of consoles. At 17 consoles, the load passes the 50% mark of the database processor utilization.

Due to the impact on the database server, Microsoft limits the total number of management group consoles to 15 concurrently active consoles. The design should clearly specify who will use which consoles so as to stay within the performance limitations. If more than 15 consoles are needed, it may indicate a requirement for multiple management groups.

Another alternative is directing those needing access to information to view reports rather than using the consoles. Reports can be pregenerated and posted on a website, reducing the impact on your MOM infrastructure.

Servers, Applications, Management Packs

As part of the assessment phase you should have collected a list of servers to monitor with MOM. This list should also include installed applications and where those are physically located. You can now use your management group design to match the servers and their applications with an appropriate management group and management server.

As an example, Coyote's servers in New York are being split between two management groups: OperatingSystems and Applications. The OperatingSystems management group

will monitor 100 servers in the New York location but will only monitor the base operating system. A single Management Server, OSMonitor01, will be used for the OperatingSystems management group. The Applications management group will monitor 50 servers in the New York location, monitoring the IIS and BizTalk functionality. A single management server, AppMonitor01, was identified for this management group.

The applications monitored by each group are used to identify the management packs those groups will deploy. The OperatingSystems support group will use the Windows Server Base Operating System (OS) management pack and the Dell and HP hardware management packs because this support group also monitors hardware functionality. The Applications support group selected the IIS and BizTalk Server 2004 management packs and is investigating adding a third-party management pack for monitoring their SAP servers.

For Contoso, two management groups are being monitored: DallasMgmt in Dallas and ChicagoMgmt in Chicago. Based on their organization's business requirements, monitoring Microsoft Active Directory is a high-priority item. Contoso has decided to use multiple management packs including Windows Active Directory, DNS, Windows File Replication Service (FRS), Dynamic Host Configuration Protocol (DHCP), Windows Server Base OS, and the Management Pack Notifier.

As part of the design, each server is identified and associated with its location and the management server it will use. The design should also include the management packs you plan to deploy.

Other Design Aspects

You will also want to consider security, alert notification, reporting, and deploying agents in designing your MOM 2005 deployment.

Security

MOM 2005 utilizes multiple service accounts to help increase security by utilizing lower privileged security accounts. Chapter 11, "Securing MOM," discusses how to properly secure your MOM environment. MOM uses several accounts that are typically Domain User accounts:

- A database connectivity account
- A MOM "action" account
- A MOM reporting account

Reducing Security Privileges for the Action Account in Windows 2003

The Action account is defined on the management server and the agent. Windows Server 2003 systems have the capability to use a low-privileged account for the Agent Action account, although Windows 2000 requires that the Agent Action account be a member of the local Administrators group. Security requirements for the Agent Action

account in a low-privileged scenario on Windows 2003 will vary based on the management packs implemented on each monitored system.

Later chapters of this book that discuss using specific management packs often will include the particular security requirements for implementing the management pack with reduced security privileges. For additional security details on management packs, we suggest you check the related Management Pack Guide.

User Notifications

MOM's functionality includes the capability of notifying users or groups as issues arise within your environment. For design purposes you should document who needs to receive notifications and for what they need to receive notifications. MOM creates notification groups as part of the initial installation and adds more groups as management packs are installed. These groups contain operators that are defined as a specific user or groups contacted via email, pager, or using a batch script. For example, if your organization has a team that supports email, they will most likely want notifications if issues occur within the Exchange environment.

Notification Workflow Solution Accelerator

MOM's notification functionality can be increased by deploying the Notification Workflow Solution Accelerator, which is discussed in Chapter 19.

Reporting

MOM 2005 includes a robust reporting solution. With MOM Reporting installed, MOM 2005 calls a Data Transformation Services (DTS) package that moves records from the OnePoint database and transfers them into the SystemCenterReporting database. The reporting database retains information for 395 days by default, configurable (roughly 13 months), which you can use as tracking information for comparison purposes. If you plan to use MOM 2005's reporting capabilities we recommend you install the reporting components prior to installing any management packs. Management packs contain reports, and the reports are not added to MOM if the reporting component is not installed. If MOM Reporting is installed later, you will have to then install the management pack reports to add the reporting functionality.

Agents

Agents are deployed onto the systems that MOM monitors. These agents can be deployed manually or automatically from the MOM Administrator console. Deploying agents from the Administrator console is recommended because it is the quickest and most supportable approach. Manual agent deployment is most often required when the system is behind a firewall, there is a need to limit bandwidth available on the connection to the management server, or if a highly secure server configuration is required. Chapter 9 provides more detail on this topic.

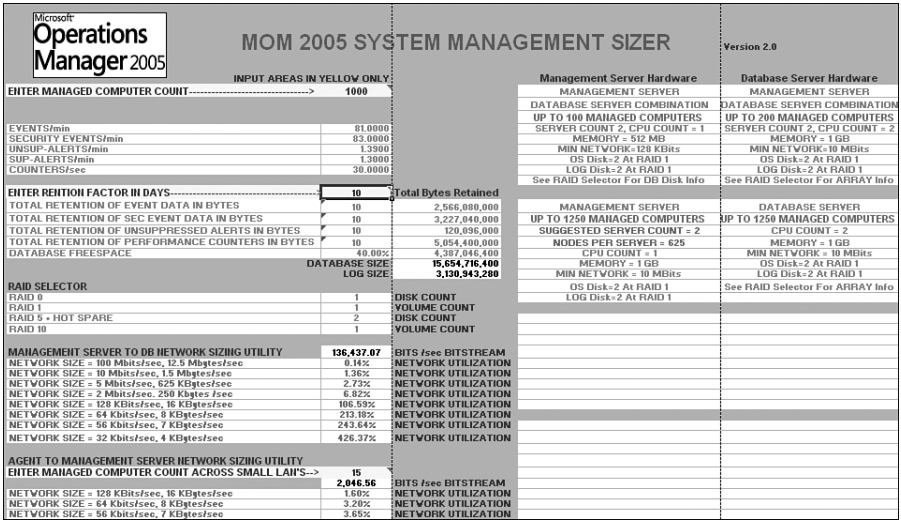
Tools to Assist with Your Design

The general rule is to keep your design simple. Just because MOM can be installed on a dozen servers doesn't mean that it should be. Several tools are available from Microsoft to assist with designing your MOM environment:

- The MOM 2005 Sizer—The MOM Sizer is available from Microsoft's Download Center. At www.microsoft.com/downloads, search for "MOM 2005 Sizer." The MOM Sizer, shown in Figure 4.2, is a Microsoft Excel spreadsheet that provides recommendations for your environment when planning what servers are necessary and their hardware requirements. You can use this information as a starting point; your design will be validated during the Proof Of Concept (POC) and pilot phases.

Performance and Sizing Paper from Microsoft

You can check the "Microsoft Operations Manager 2005 Performance and Sizing" whitepaper to help you to determine the appropriate performance and sizing considerations for MOM 2005 in your specific environment. This can be accessed at http://go.microsoft.com/fwlink/?linkid=47141 or downloaded from http://www.microsoft.com/downloads; search for "MOM 2005 Performance and Sizing Guide."



Microsoft Operations Manager 2005

MOM 2005 SYSTEM MANAGEMENT SIZER

Version 2.0

INPUT AREAS IN YELLOW ONLY

			Management Server Hardware	Database Server Hardware
ENTER MANAGED COMPUTER COUNT---------->	1000		MANAGEMENT SERVER	MANAGEMENT SERVER
			DATABASE SERVER COMBINATION	DATABASE SERVER COMBINATION
			UP TO 100 MANAGED COMPUTERS	UP TO 200 MANAGED COMPUTERS
EVENTS/min	81.0000		SERVER COUNT 2, CPU COUNT = 1	SERVER COUNT 2, CPU COUNT = 2
SECURITY EVENTS/min	83.0000		MEMORY = 512 MB	MEMORY = 1 GB
UNSUP-ALERTS/min	1.3900		MIN NETWORK=128 KBits	MIN NETWORK=10 MBits
SUP-ALERTS/min	1.3000		OS Disk=2 At RAID 1	OS Disk=2 At RAID 1
COUNTERS/sec	30.0000		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
ENTER RENTION FACTOR IN DAYS---------->	10	Total Bytes Retained		
TOTAL RETENTION OF EVENT DATA IN BYTES	10	2,566,080,000	MANAGEMENT SERVER	DATABASE SERVER
TOTAL RETENTION OF SEC EVENT DATA IN BYTES	10	3,227,040,000	UP TO 1250 MANAGED COMPUTERS	UP TO 1250 MANAGED COMPUTERS
TOTAL RETENTION OF UNSUPPRESSED ALERTS IN BYTES	10	120,096,000	SUGGESTED SERVER COUNT = 2	CPU COUNT = 2
TOTAL RETENTION OF PERFORMANCE COUNTERS IN BYTES	10	5,054,400,000	NODES PER SERVER = 625	MEMORY = 1 GB
DATABASE FREESPACE	40.00%	4,387,046,400	CPU COUNT = 1	MIN NETWORK = 10 MBits
DATABASE SIZE		15,654,716,400	MEMORY = 1 GB	OS Disk=2 At RAID 1
LOG SIZE		3,130,943,280	MIN NETWORK = 10 MBits	LOG Disk=2 At RAID 1
RAID SELECTOR			OS Disk=2 At RAID 1	See RAID Selector For ARRAY Info
RAID 0	1	DISK COUNT	LOG Disk=2 At RAID 1	
RAID 1	1	VOLUME COUNT		
RAID 5 + HOT SPARE	2	DISK COUNT		
RAID 10	1	VOLUME COUNT		
MANAGEMENT SERVER TO DB NETWORK SIZING UTILITY	136,437.07	BITS /sec BITSTREAM		
NETWORK SIZE = 100 Mbits/sec, 12.5 Mbytes/sec	0.14%	NETWORK UTILIZATION		
NETWORK SIZE = 10 Mbits/sec, 1.5 Mbytes/sec	1.36%	NETWORK UTILIZATION		
NETWORK SIZE = 5 Mbits/sec, 625 KBytes/sec	2.73%	NETWORK UTILIZATION		
NETWORK SIZE = 2 Mbits/sec, 250 Kbytes /sec	6.82%	NETWORK UTILIZATION		
NETWORK SIZE = 128 KBits/sec, 16 KBytes/sec	106.59%	NETWORK UTILIZATION		
NETWORK SIZE = 64 Kbits/sec, 8 KBytes/sec	213.18%	NETWORK UTILIZATION		
NETWORK SIZE = 56 Kbits/sec, 7 KBytes/sec	243.64%	NETWORK UTILIZATION		
NETWORK SIZE = 32 Kbits/sec, 4 KBytes/sec	426.37%	NETWORK UTILIZATION		
AGENT TO MANAGEMENT SERVER NETWORK SIZING UTILITY				
ENTER MANAGED COMPUTER COUNT ACROSS SMALL LAN'S-->	15			
	2,046.56	BITS /sec BITSTREAM		
NETWORK SIZE = 128 KBits/sec, 16 KBytes/sec	1.60%	NETWORK UTILIZATION		
NETWORK SIZE = 64 Kbits/sec, 8 KBytes/sec	3.20%	NETWORK UTILIZATION		
NETWORK SIZE = 56 Kbits/sec, 7 KBytes/sec	3.65%	NETWORK UTILIZATION		

FIGURE 4.2 The MOM Sizer.

On the CD

You can find the MOM 2005 Sizer on the CD included with this book.

- The System Center Capacity Planner—This tool (see Figure 4.3), can be used to assist in architecting a MOM solution and provides the ability to create "what-if" analysis, such as "what-if" I add another 100 servers to be monitored by MOM 2005?

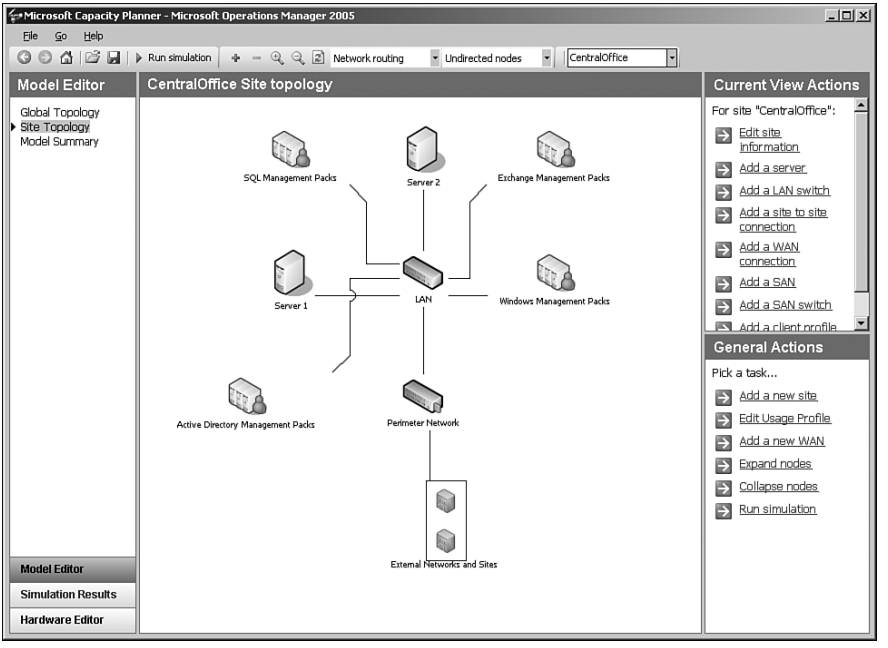


FIGURE 4.3 System Center Capacity Planner.

To complete the design phase, each of the aspects discussed needs to be Documented, Discussed, Revised, and Agreed upon, or "DDRA." Following this process identifies potential issues with the design before it is tested in proof of concept, facilitates communication with other members of your organization, and helps drive acceptance of MOM 2005 within your company.

In the next few sections we will provide sample designs for a single server configuration and then review a multiple server MOM configuration.

Designing a Single MOM Server Configuration

Sometimes the scalability Microsoft builds into its products makes it challenging to see how to deploy a simple solution. We will cut through that and show you where you can deploy a simple single server solution.

MOM was specifically designed to scale from the smallest office to the largest, worldwide enterprises. Consequently, decisions must be made as to the size and placement of the MOM servers. As part of the design process, an organization must decide between implementation with a single server or a deployment onto multiple servers. Understanding the criteria defining each design scenario aids in selecting a suitable match.

As with many other technical systems, the simplest configuration meeting your needs can work the best and cause the fewest problems. This is also true of MOM; many smaller-sized organizations can design a MOM solution comprised of a single MOM server. Certain conditions need to be present in your infrastructure to make optimal use of a single server MOM installation. If the following conditions are present, this type of design scenario may be right for your organization:

- Monitoring less than 100 servers
- Maintaining one year of stored data

Generally, a single MOM server configuration works for smaller to medium-sized organizations and particularly those who prefer to deploy MOM to smaller, phased groups of servers. Another advantage of MOM's architecture is its flexibility to changes in a design scope. You can add additional MOM component servers to a configuration later without the worry of major reconfiguration.

Single Server Requirements

Figure 4.4 shows the single server configuration with all the roles collapsed onto a single server.

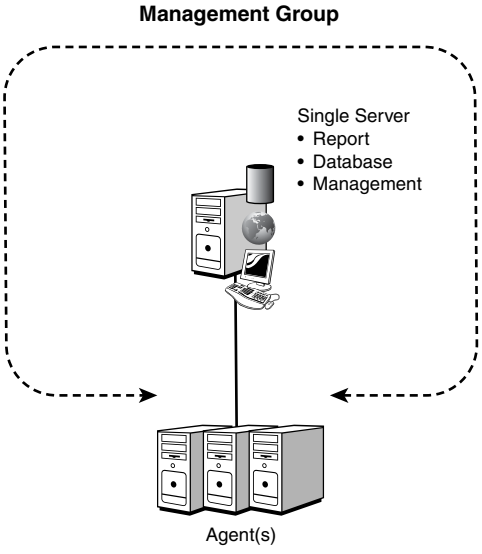


FIGURE 4.4 Single server configuration.

Assuming an average level of MOM activity, your single MOM server should be a single processor 2.4GHz P4 or higher and 1GB of memory to achieve optimal results (shown in Table 4.11). The goal is to avoid taxing your processor by having a sustained CPU utilization rate of more than 75%. Consequently, a configuration of fewer than 100 managed nodes should not exceed this threshold using the proper hardware. Ensure that the tests

that you perform include any management packs that you might add to MOM because these management packs can easily add 25% to your MOM server CPU utilization.

TABLE 4.11 Single Server Hardware Specification

Hardware	Requirement
Processor	2.4GHz P4
RAM	1GB
Hard disk	250GB
CD-ROM	Needed
Display adapter	Super VGA
Monitor	1024x768 Resolution
Mouse	Needed
Network	100Mbps

Based on a standard growth rate of 5MB per managed computer per day, which we will see in the "Operations Database Sizing" section later in this chapter, the total space for the year of stored data will be 100 agents * 5MB / day * 365 days = 182,500MB, or approximately 200GB. The operations database in this configuration is set to retain data for 7 days, which translates to 100 agents * 5MB / day * 7 days = 3,500MB, or approximately 4GB. The operations database can grow to 30GB, so it is prudent to allocate enough space for it to grow to that size. Approximating once again, we arrive at 250GB total space required. Table 4.12 lists a variety of drive sizes, the RAID configuration, and the usable space. Table 4.12 assumes that the number of drives includes the parity drive in the RAID, but not an online hot spare.

TABLE 4.12 Single Server Drive Configuration

Drive Size	Number of Drives	Configuration	Usable Space
36GB	8	RAID5	252GB
72GB	5	RAID5	288GB
146GB	3	RAID5	292GB
300GB	2	RAID1	300GB

It is always recommended to place the database on a disk array separate from the operating system because I/O saturation can occur when they are combined. MOM also works best on a 100Mb (or 1Gb) network and should be connected to a switch (preferably on the backbone with other production servers).

Single Server Configuration

In the single server configuration, the server contains all components of the typical MOM installation, including the management server and reporting server. See Chapter 6, "Installing MOM 2005," for the specific installation steps.

Designing a Multiple MOM Server Configuration

Although it is often simpler to install a single MOM server to manage your server infrastructure, it may become necessary to deploy multiple management servers if you need to perform any one of the following functions in your environment:

- Monitor more than 100 servers.
- Collect and report on more than a month or two of data.
- Add redundancy to your MOM environment.
- Monitor computers across a WAN or firewall.
- Segment the MOM database onto another server.

In multiple-server configurations, MOM components are typically broken into the three different server roles. These roles are management server, database server, and report server. Each environment can have more than one of these servers depending on the needs of the organization:

- Database server role—The database server normally contains the operations database and is a platform optimized for data collection—that is, to rapidly process a large flow of incoming data from the management servers. In classic client server architecture, this would be the backend tier. In the MOM architecture, this is a big portion of the data layer or tier.
- Management server role—The management server typically contains the management service, the DAS, an agent, the Administrator console, the Operations console, and the Web console. The management server thus handles most of the centralized business logic and presentation layer functions, with the important exception of the reporting functions. Of course, a large measure of business logic is executed locally by the agents on the managed computers.
- Report server role—The report server typically contains the reporting database and the Reporting console. This is frequently separated into a separate server for performance reasons, allowing large volumes of data to be retained and mined using the reporting function without impacting the operations function running on the database and management servers.

The management group encompasses a single instance of a database server role and a single instance of a report server role but can include multiple management servers. These server roles are all components of a management group as discussed in Chapter 3, "How Does It Work?"

Multiple Server Requirements

It is generally a good practice to include high levels of redundancy into any mission-critical server, such as management servers, MOM consoles and database servers. It is therefore recommended to include as many redundant components into your server hardware design and to choose enterprise-level servers whenever possible.

Disk space for the database server is always a consideration. As with any database, the MOM database can consume vast quantities of drive space if left unchecked. Luckily, it is limited to 30GB by Microsoft for supportability reasons. We recommend that your operations database server contain a minimum of 50GB free disk space and possibly more, depending on how many nodes you will be monitoring and how long you want to keep the data. The extra space allows for database operations such as backups and restores, as well as emergency growth of the operations database. In addition, backups of the entire database on a regular basis are a must.

The report server can be configured similar to the database server, but will require a much larger storage capacity. Whereas the operations database typically stores data for a period of days, the report server typically stores the data for a year. This data can grow rapidly and is discussed in the "Designing MOM Sizing and Capacity" section later in this chapter.

Placement of the Management Servers

Management servers can be placed close to their database servers or close to the agents they manage. Several key factors can play roles in determining where the servers will reside, however. These factors are listed as follows:

- Maximum bandwidth between components—MOM servers should have fast communication between all components in the same management group to maximize the performance of the system. The management server needs to be able to upload data quickly to the database server. This usually means T1 speed or better, depending on the number of agents the management server is supporting.
- Redundancy—Adding additional management servers increases the failover capability of MOM and helps to maintain a specific level of uptime. Depending on your organization's needs, additional servers can be built into your design as appropriate.
- Scalability—If a need exists to expand the MOM environment significantly or to increase the number of monitored servers with short notice, additional MOM management servers can be established to take up the slack.

In most cases, you can centralize the management servers in close proximity with their database server and allow the agents to communicate with the management servers over any slow links that might exist.

As a rule, for multiple server MOM configurations, you should have at least two management servers for redundancy.

Using Multiple Management Groups

As defined in Chapter 3, MOM management groups are composed of a single SQL Server operational database, a single report server, a unique name, and one or more management servers. Each management group uses its own database and is configured separately from other management groups.

It is important to note that agents can be configured to report to multiple management groups and that alerts can be forwarded between management groups. This increases the flexibility of the system and allows for the creation of multiple management groups based on your organization's needs. There are four major reasons for dividing your organization into separate management groups:

- Geographic or bandwidth-limited regions—Similar in approach to Windows 2003 sites or Exchange 2003 routing groups, MOM management groups can be established to segregate network subnets to reduce network bandwidth consumption. It is not recommended to span management groups across slow WAN links because this can lead to link saturation and your company's network support team hunting you down in the parking lot. Aligning the creation of management groups based on geographic or bandwidth criteria is always a good idea.

  If the size of the remote office does not warrant creating a new management group, MOM should be configured to throttle the event monitoring schedule to avoid peak usage times. For example, a site with fewer than 10 servers typically does not warrant its own management group. The downside to this is a potential delay in notification of critical events.

- Functional or application level control—This is a useful feature of MOM 2005, where a single agent can be managed by multiple management groups. The agent keeps the rules that it gets from each of the management groups completely separated and can even communicate over separate ports to the different management groups.

- Political or business function divisions—Although not as common a solution as bandwidth-based management groups, political boundaries can also be aligned with MOM management group boundaries. This would normally only occur if there was a particular need to segregate specific monitored servers onto separate zones of influence. For example, the Finance group's servers could be monitored in their own management group to lessen the security exposure that their servers receive.

- Very large numbers of agents—In a nutshell, if your management group membership approaches the limitation's number of monitored servers, it is wise to segment the number of agents into multiple management groups to improve network performance. This is appropriate when the number of managed computers approaches 4,000, or the database size approaches Microsoft's supportability limits.

To illustrate this point using the bandwidth-limited criteria, if your organization is composed of multiple locations separated by slow WAN links, it would be wise to separate each location not connected by a high-speed link into a separate management group and enable alert forwarding between the management groups.

Another example is when IT support operations are functionally divided into a platform group (managing the Windows operating system) and a messaging group (managing the Exchange application), two management groups might be deployed (a platform management group and a messaging management group). This would allow the platform group

to have complete administrative control over its management infrastructure while also allowing the messaging group to have complete administrative control over its management infrastructure. The two groups would jointly operate the agent on the monitored computers.

The MOM Database—Placement and Issues

Keeping in mind that each management group has a separate database, it must also be noted that, as opposed to management servers, only one SQL Server database instance can run in each management group. Consequently, each SQL Server installation should be placed and configured with the following factors kept in mind:

- Network bandwidth—As with the other MOM components, placing the MOM SQL database component on a dedicated switch, gigabit backbone, or other fast connection that can communicate freely with the MOM management servers is key. Slow network performance can significantly affect the capability of MOM to respond to network conditions.
- Hardware redundancy—Most enterprise server hardware contains contingencies for hardware failures. Redundant fans, RAID mirror sets, dual power supplies, and the like all help to ensure the availability and integrity of the system. SQL Server databases especially need this level of protection because they must be gracefully shut down to preserve their integrity.

  Where high availability is needed, the database can be clustered and/or replicated to provide redundancy and failover capabilities.
- SQL Server licensing—Because SQL Server is a separate licensing component from Microsoft, each service account that accesses the database must have its own Client Access License (CAL). That means that if there is a separate service account for the DAS and Consolidator, two CALs must be purchased.

  Licensing can be an important cost factor if clustering or replication is chosen and depends on the SQL Server edition installed.

Generally, the MOM database server is placed in close proximity with the MOM reporting server. There will be significant data transfer between the two components on a daily basis by the DTS package that transfers the operations database data into the reporting database. This can have a big impact on WAN links.

Designing MOM Sizing and Capacity

Although MOM contains multiple mechanisms to allow it to scale to large environments, several limitations to the software must be taken into account if your environment is subject to them. The number of agents you deploy and the amount of data you want to share directly impact capacity limitations and the size of your database. A better understanding of exactly what MOM's limitations are can help better define what design to utilize.

Data Flows in MOM

Data flow in MOM 2005 is an important design consideration. In a typical MOM 2005 environment there is a large quantity of data flowing from a relatively small percentage of sources within the IT environment. These data flows are latency sensitive, due to needing alerts and notifications in a short time frame that is measured in seconds.

The data flowing from each agent is not that great when considered individually, being on the order of 0.5 Kbps. However, when looked at in aggregate for a large number of servers, the load can be significant as shown in Table 4.13, which shows the estimated minimum bandwidth for just the Windows Operating System Base Management Pack. Using Table 4.13, you can see that the need for multiple 100 Mbps or Gigabit network cards becomes important above the 500 agent mark.

TABLE 4.13 Management Server Aggregate Bandwidth for Agents

Agents	Total Kbps	Utilization of a 100 Mbps NIC
1	0.50	0%
5	2.50	0%
10	5.00	1%
100	50.00	5%
500	250.00	25%
1000	500.00	50%

The data flow can be adjusted in two ways:

- How often the agents upload their data
- How much data is uploaded

For low bandwidth agents, you can consider adjusting the settings for heartbeat and data upload times, but this will *not* reduce the overall volume of information. More information will be uploaded at less frequent intervals, but it will be the same quantity of data. To reduce the data volume, you need to adjust the rules to collect less data. As an example, adjusting the sample interval of a performance counter from 15 minutes to 30 minutes will reduce the volume of data by half.

Limitations, Provisos, and Restrictions

Management servers, management groups, and collections of management groups have some inherent limitations. These limits are in some cases hard limits that cannot be technically broken (such as the tiered structure) and in others are supportability limits that should not be broken. Microsoft tests and supports its products but sets limits on the scale of the systems that reflect the limits of the testing and support. Table 4.14 summarizes the capacity limitations for MOM 2005 components. Although MOM includes implicit design components that allow it to scale to large groups of managed nodes, there are some maximum levels that could limit the size of management groups.

TABLE 4.14 Limitations Summary as of MOM 2005 SP1

Area	Limitation Description	Limit
Management Group	Maximum agents per management group	4,000
	Maximum agentless computers per management group	60
	Maximum management servers per management group	10
	Maximum reporting servers per management group	1
Management Server	Maximum agents per management server	2,000
	Maximum agentless computers per management server	10
	Maximum consoles per management server	15
Agent	Maximum management servers per agent	4
Database	Maximum size of operations database	30GB
	Maximum size of reporting database	200GB
Tier	Maximum destination management groups	1
	Maximum source management groups	10
	Maximum management groups tiers	3
	Maximum alert forwards per day per destination management group	400,000

The table is organized by the area of the limitation. Even though there is a stated limit, in a given environment the limit might not be practical. For example, the maximum number of agents per management server is 2,000. However, a single management server is unlikely to be capable of supporting 2,000 Exchange servers due to the particularly heavy load these agents place on a management server.

Many of these capacity limitations are actually supportability limitations rather than hard technical limitations. For example, launching a 16th console will not generate an error or alert. Exceeding the limitations will not immediately cause the system to fail but will rather start to impact performance, latency, and throughput of the MOM infrastructure. For this reason, Microsoft imposes these limitations from a supportability perspective and does not guarantee that the MOM 2005 product will function properly if they are exceeded.

Doing the Math

If you do the math, you can see that each management group will architecturally support a maximum of 4,000 agents. You will also notice that you can have only a single destination management group, and you can have at most 10 source management groups in a two-tiered architecture; then you can support at most 44,000 managed computers in a single cohesive MOM 2005 infrastructure. This is based on the following equation:

```
4,000 agents / MG x (10 source MG + 1 destination MG) = 44,000 agents
Where MG = Management Group
```

Because MOM's intent is to monitor primarily servers, being able to scale to *only* monitor 44,000 servers is not much of a limitation for the vast majority of organizations!

Even though the capacity limitations outline the maximums for the MOM architecture, typically constraints such as storage, network throughput, and geopolitical issues place even stricter limitations on the capacity of the MOM infrastructure. The next two sections on database sizing illustrate one of the more compelling constraints.

Operations Database Sizing

Sizing the MOM database can be a complex endeavor. Several factors must be taken into account, and a complex formula exists for calculating database size. We suggest purchasing a large quantity of disk space for your MOM database. If space limitations are an issue, it is possible to reduce the size of the database through regular database grooming. By doing some MOM Math, you can calculate the database size if you know the following information and apply it to the formulas in Table 4.15.

TABLE 4.15 Database Daily Growth Formulas

Data Type	Formula
Alerts size in DB	Alerts/day x alert size
Events size in DB	Events/day × event size
Event parameter size in DB	Events parameters/day × parameter size
Performance size in DB	Performance counters/day × counter size × time

It may seem complicated, but these equations simply measure the database size used by MOM based on how many alerts you receive, the events you receive, and how many counters are measured and how large they are. The formulas give the database growth for a single computer per day. To get the estimated daily growth, add the results of each of the formulas. It turns out that to a close order of approximation, you can safely ignore the alerts component because it is relatively small.

In practice, few people actually know the values for the previous variables, and it is often easier to throw disk space at a MOM database server than to sit in front of a chalkboard doing the math for this equation.

The general database space consumption for alerts, events, and performance data are provided in Table 4.16.

TABLE 4.16 Average Values for Data Sizes

Data Type	Average Size
Alert size	2,606 bytes
Event size	1,313 bytes
Event parameter size	72 bytes
Performance size	217 bytes

Based on extensive research done in practice in the field, a MOM 2005 system produces the quantities shown in Table 4.17 for each managed computer. These are realistic numbers, but the deployment of different management packs, tuning, and customizations can have a major impact on these numbers.

TABLE 4.17 Average Rates of Occurrence Per Agent Per Day

Data Type	Count Per Day
Alerts	4
Events	208
Event parameters	849
Performance	13,976

The combination of these two factors results in the growth rate of approximately 3.37MB per day per agent. Table 4.18 shows the specific calculations based on the formulas.

TABLE 4.18 Average Daily Database Growth

Data Type	Formula	Bytes Per Day	Percentage
Alerts size in DB	4 alerts per day x 2,606 bytes	10,424	0.30%
Events size in DB	208 events per day x 1,313 bytes	273,104	8.09%
Event parameter size in DB	849 event parameters x 72 bytes	61,128	1.81%
Performance size in DB	13,976 performance measurements x 217 bytes	3,032,792	89.90%
Total		3,377,448	100.00%

You may have noted that in our server design examples, we used a figure of 5MB per day. For purposes of estimation, the general rule of thumb is to use a figure of 5MB per agent per day to allow for a margin of error.

Figure 4.5 shows the proportion of growth for each of the four major data types. As you can see from the chart, the performance data vastly overwhelms the other data. Alerts, although being a large data type, are so few in number that they barely register.

With the growth rates shown in Table 4.18, the size of the database will be determined by the number of days that the data is retained in the operations database—that is, the grooming interval. The default grooming interval is four days, and those values are italicized in Table 4.19. The operations database is limited to 30GB total by Microsoft for supportability reasons, but 40% needs to be available for reindexing and other housekeeping operations, making the data limit really 18GB. The values in Table 4.19 that exceed the supported limit are highlighted in bold in the table.

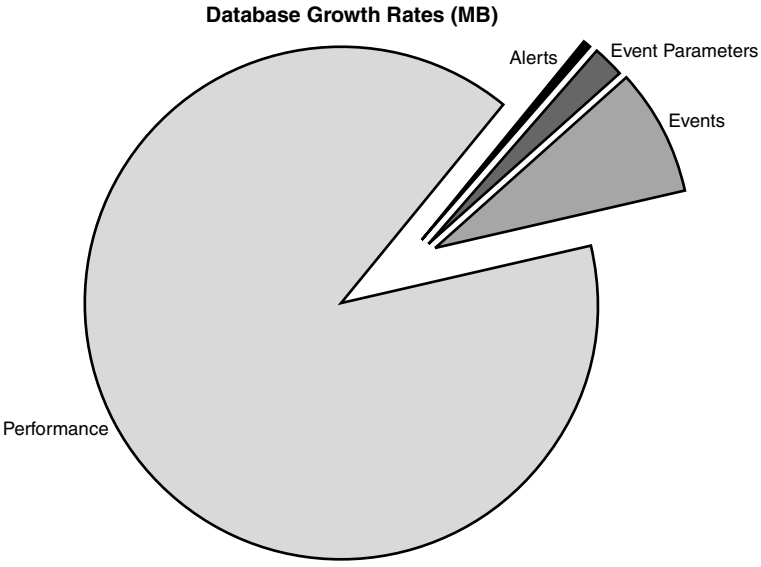


FIGURE 4.5 Database growth rates per agent in MB.

TABLE 4.19 Operations Database Sizes in MB for Various Grooming Intervals and Agents

Grooming Interval (days)	Growth Rate (MB/day)	10 Agents	50 Agents	100 Agents	500 Agents	1,000 Agents	2,000 Agents	4,000 Agents
1	5	50	250	500	2500	5000	10000	**20000**
2	5	100	500	1000	5000	10000	**20000**	**40000**
3	5	150	750	1500	7500	15000	**30000**	**60000**
4	5	*200*	*1000*	*2000*	*10000*	***20000***	***40000***	***80000***
5	5	250	1250	2500	12500	**25000**	**50000**	**100000**
6	5	300	1500	3000	15000	**30000**	**60000**	**120000**
7	5	350	1750	3500	17500	**35000**	**70000**	**140000**
14	5	700	3500	7000	**35000**	**70000**	**140000**	**280000**
30	5	1500	7500	15000	**75000**	**150000**	**300000**	**600000**
45	5	2250	11250	**22500**	**112500**	**225000**	**450000**	**900000**

As you can see from Table 4.19, the default grooming interval of four days will not support 1,000 agents based on the database size. At 1,000 agents, the default grooming interval results in a database size of 20GB, which would not be supported by Microsoft. To support 1,000 agents, the grooming interval would have to be set to three days or less.

Figure 4.6 charts the growth of the database for ease of reference. The series lines for each of the agent counts plot the projected size of the operations database for the given grooming interval. You can see the projected growth of the operations database as the grooming interval is increased. To remain within supportability guidelines, the chart lines should remain below the 18,000MB (18GB) horizontal line. For 2,000 agents, clearly the grooming interval has to be set at 1 day whereas for 50 agents you could set the grooming interval to 45 days without a problem.

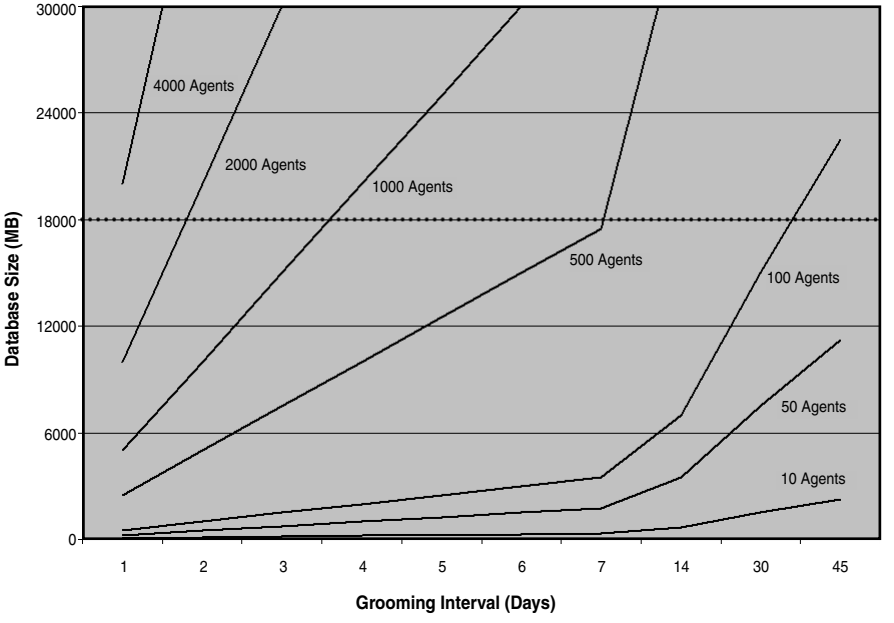


FIGURE 4.6 Operations database size chart.

Tuning Needed at the Maximum Number of Agents

If you have the maximum number of agents that MOM supports in a single management group, the projected operations database size for the lowest grooming interval possible exceeds the supported size of the database. For 4,000 agents, the projected operations database size with a grooming interval of one day will be 20GB. This exceeds the 18GB limit imposed by Microsoft.

When deploying to such a large number of agents in a single management group, you would need to aggressively tune the rules to collect less than the standard volume 5MB per agent per day of data.

These estimates were made assuming a standard deployment of MOM 2005 with the standard management packs configured in a standard manner. Because no deployment of MOM is actually "standard," it is important to conduct appropriate testing and monitor

growth rates of your installation over time. Your growth rate may vary from the 5MB per day per agent used here.

Speaking of varying the growth rate of the database, Figure 4.5 gives you a clear indication of where to tune if you need to limit the growth of the database. Performance measurements are by far the largest portion of the database growth rate, making it a likely area for tuning to reduce database growth.

Reporting Database Sizing

The reporting database is the long-term repository of the data. Database growth is the same as the operations database, but the retention interval is longer. By default, the data is kept in the reporting database for 395 days, or about 13 months. The Microsoft supportability limit was at one point 1TB (1,000,000MB), but this is based on reporting latency and only what they tested. There is no hard limit other than time to generate a report.

Microsoft has a management pack designed to manage latency called the MOM 2005 Summary Reporting Pack (SRP). The SRP provides weekly and daily summarization of data with a variety of reports. We discuss the SRP in the next section, "Using the MOM 2005 Summary Reporting Pack."

Table 4.20 shows the reporting database size for various grooming intervals and agent counts. The reporting database sizes that fall outside the supportability limits are highlighted in bold.

TABLE 4.20 Reporting Database Sizes in MB for Various Grooming Intervals and Agents

Grooming Interval	Growth Rate	10 Agents	50 Agents	100 Agents	500 Agents	1,000 Agents	2,000 Agents	4,000 Agents
1 Month	5	1500	7500	15000	75000	150000	300000	600000
2 Month	5	3000	15000	30000	150000	300000	600000	**1200000**
1 Qtr	5	4562	22812	45625	228125	456250	912500	**1825000**
2 Qtr	5	9125	45625	91250	456250	912500	**1825000**	**3650000**
3 Qtr	5	13687	68437	136875	684375	**1368750**	**2737500**	**5475000**
1 Yr	5	18250	91250	182500	912500	**1825000**	**3650000**	**7300000**
5 Qtr	5	22812	114062	228125	**1140625**	**2281250**	**4562500**	**9125000**
6 Qtr	5	27375	136875	273750	**1368750**	**2737500**	**5475000**	**10950000**
7 Qtr	5	31937	159687	319375	**1596875**	**3193750**	**6387500**	**12775000**
2 Yr	5	36500	182500	365000	**1825000**	**3650000**	**7300000**	**14600000**

As you can see from Table 4.20, the default grooming interval of one year will support up to about 500 agents, assuming standard database growth rates. A picture is worth a thousand words, so we show the same information in Figure 4.7. Because the chart lines should not cross the 1,000,000MB (1TB) horizontal line, you can readily see that the maximum agent count of 4,000 will only support about a month of data.

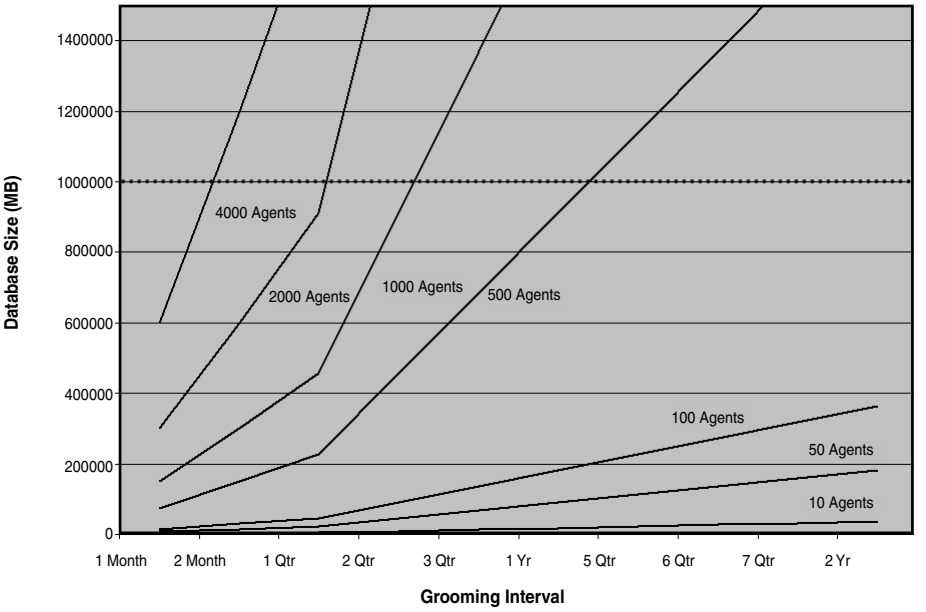


FIGURE 4.7 Reporting database size chart.

When estimating the size of the reporting database it is important to consider the amount of data collected daily and how long you intend to keep the data in the reporting database because this will directly affect your storage requirements. Your POC should provide good figures for projecting the size of the reporting database and transaction log file.

The following formula can be used to calculate the storage requirements of the reporting database. The formula states to monitor how much data is collected through your MOM environment per day and then multiply that number by the number of days you intend to keep the data. The result then needs to be doubled to account for the additional space the reporting database needs to keep track of everything in the database, such as indexes.

```
(Size of data/day x Retention Days) x 2 = SystemCenterReporting Database
```

In addition to the database requirements, you must ensure that enough free space exists in the reporting database transaction log file. The transaction log file is required to store data temporarily while the DTS job transfers data from the operations database to the reporting server. The following formula can be used to calculate the storage requirements of the reporting database transaction log:

```
Size of data/day x 5 = SystemCenterReporting Transaction Log
```

The MOM reporting database uses a database recovery mode set to simple, meaning that after the transfer of data from the operations database is complete, the data in the transaction log is removed, and the space is automatically recovered.

For both the operations database and the reporting database, the sweet spot seems to be 500 agents with the default grooming intervals and the standard management packs. That is a good design point of reference. If you needed to support 1,000 agents, adjusting the operations database grooming interval to three days and the reporting database grooming interval to six months would keep the design within the Microsoft supportability specifications.

If limiting the data is not an option, there are several potential solutions to manage this data volume:

- Extract the data to reports—A simple method is to simply generate monthly reports of the data and archive those reports for as long as the data is needed. These reports in effect summarize and distill the important data. You can even export them to Excel spreadsheets or .csv files for later use. The trade-off is lack of flexibility in generating new reports from the data.
- Reduce the time interval—Although keeping data for a year might be nice, it may be sufficient to have only a quarter or so of reporting database data online to generate reports. If that horizon is sufficient and brings you within the supportability limits, it is an easy solution.
- Create archive snapshots—If you need access to the data and cannot accept a shorter window of time, another option is to create separate snapshots of the database every month or every quarter. These can be archived to tape and restored to a temporary database when needed. The data source for the reports is simply redirected to the temporary database to generate reports. See Chapter 21 for details on archiving and changing the data source. Caveats are some administrative difficulty in restoring the databases when reports need to be generated, some tape storage is needed, and the reports only cover the period of the snapshots.
- Distill the data—The data can be extracted from the database using DTS in summarized form to retain the essence of the information with fewer granularities. For example, processor utilization has sampled values for each processor and the total for every 15 minutes. Stored for a year for a dual processor system, this would be 105,120 data points and about 23MB of storage. If this is summarized as a daily average of the total processor utilization, the data collapses down to 365 data points and about 79KB of storage. That is a 288:1 ratio of data reduction, which is pretty good. This requires some development work to create the extraction routines, a separate database for the summarized data, and custom reports to view the data.
- Multiple management groups—Multiple management groups can be used to break the data into manageable chunks. This requires additional hardware and management, and does not allow you to easily generate consolidated reports. This option is discussed in the "Multiple Management Groups" section later in this chapter.

These potential workarounds to the problem of database volume can be implemented individually or together. For example, you might create quarterly archive snapshots to

review the historical data up to one year old and use archived monthly reports to view historical data up to five years old.

Using the MOM 2005 Summary Reporting Pack

The MOM 2005 Summary Reporting Pack (SRP) helps minimize the disk space requirements for MOM Reporting. The SRP extends the MOM reporting database, providing historical reports on performance metrics and alerts. These reports are based on weekly and daily data summarizations. Reports available with the SRP Pack include the following:

- Exchange Server resource and protocol utilization
- Active Directory disk utilization and replication latency
- Operating System performance
- Generic summary reports for performance counter analysis, alert counts, and alert resolution times

The MOM 2005 SRP creates new tables in the SystemCenterReporting database used by MOM 2005 Reporting. Microsoft designed the SRP to increase performance and reduce total storage requirements for the reporting database. To determine your own size requirements, install the reporting pack in a testing environment and determine whether its functionality meets your business needs. The SRP provides historical reports for your MOM environment based on aggregated data rather than the full data collected from the OnePoint database. If the reports provide sufficient information, you can then groom the nonaggregated data in the reporting database to decrease the database size. The SRP is available at the download site http://www.microsoft.com/downloads, search for "Summary Reporting Pack." The SRP requires MOM 2005 SP1.

Sizing the Reporting Database with the SRP

To estimate space requirements with the SRP you would use the same process as before to calculate space for the MOM reporting database. For this example, we will use the same configuration that has all agents and management packs installed.

The size of the reporting database is 5GB at the start of the week. At the end of the week the reporting database is 5.35GB (increasing at 50MB/day). Based on this growth, it is possible to project that the total size of the reporting database will be approximately 24.75GB in size (5.0GB + (.05GB * 395)). Note that this example only provides a method to approach when estimating database size and may not necessarily reflect actual numbers. The formula for this example is Original OnePoint database size + (Daily size increase * Reporting Retention Period).

Management Group Scalability

MOM is capable of scaling as your monitoring environment increases to large amounts of managed nodes. Through the use of management groups, multiple management servers, and event forwarding, almost any project becomes a possibility.

Using the numbers, if the amount of nodes to be monitored is greater than 100, it is time to consider multiple management servers per management group (shown in Figure 4.8). As a general rule of thumb, every increase in 250–500 nodes should be followed by adding another management server, up to the hard limit of 10 management servers per management group.

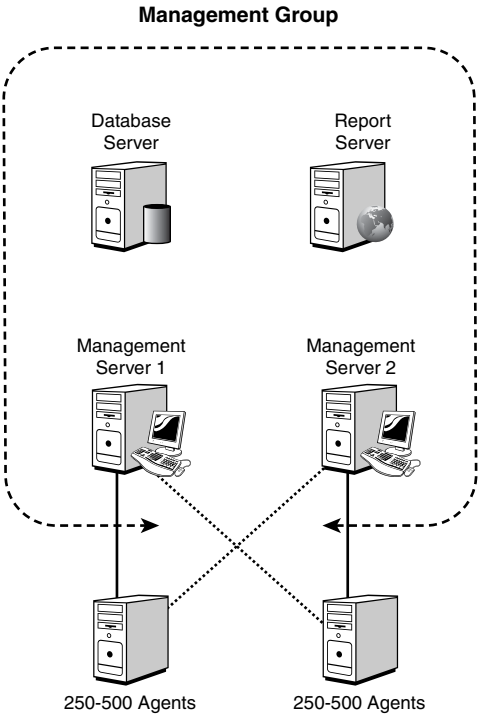


FIGURE 4.8 Multiple management servers in a management group.

Multiple Management Groups

Expanding to use multiple management groups, as we previously defined, can take place at the designer's discretion, although it is typically done to segregate different geographic areas with slow WAN links from each other. If the link speeds to remote managed nodes are under 256 Kb per second, we recommend either creating a new management group, or greatly throttling the amount of information collected from remote agents.

Determining whether to create a new management group or simply to throttle the events sent will depend on the amount of remote servers. It does not make sense to create a new management group if you have only two small sites with four servers each to monitor.

If, however, your remote servers are spread around various offices that have better connections to each other than they do to your primary management group, it may be wise to create a new management group. This would typically be the case if you were to create management groups based on continent, for example. Figure 4.9 shows a worldwide MOM 2005 infrastructure with regional management groups (North America, Europe, and Asia). The regional management groups forward their alerts using the MOM-to-MOM connector to a global management group.

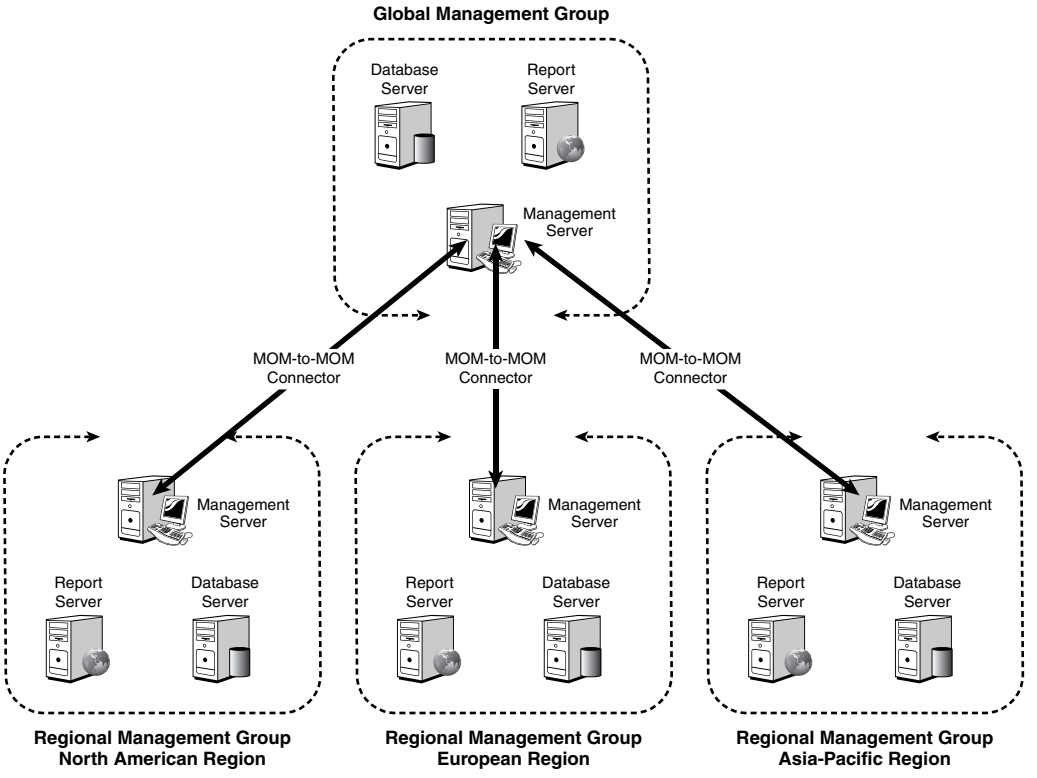


FIGURE 4.9 Management groups by geographic region.

In this configuration, each region can operate the management groups semiautonomously, yet still allow a global view of the environment worldwide using a global console.

Through creating and manipulating management groups and management servers, your MOM environment can scale from a handful of monitored servers to large numbers of nodes worldwide. This scalability helps establish MOM as an enterprise monitoring solution.

Planning

After determining your MOM 2005 design, the next step is to plan for the remaining phases, which include proof of concept, pilot, and implementation. These phases have the same goals: limiting potential risk to your production environment and avoiding "alert overload" of your organization.

Defining Risk

Any time a production environment changes there is a risk that the change can cause a problem within the environment.

It is important to try to avoid alert overload, which refers not to a technical hardware constraint but to an attention constraint on the part of the people involved with monitoring MOM who can only handle a limited number of alerts. Alert overload occurs when the number of alerts generated causes the human receivers of these alerts to either ignore the errors or actively oppose using the tool providing the notifications. You don't want to cry wolf unless there is a really good chance that there is a wolf at the door. Avoiding risk and alert overload can positively impact the likelihood of a successful MOM 2005 deployment. Your planning document should include details on your proof of concept, pilot, and implementation phases.

Proof of Concept Planning

A proof of concept (POC) should emulate the production hardware as closely as possible. Use production hardware for the MOM 2005 solution if it is available because that will most closely emulate your production environment. Isolate your POC network configuration from production to allow full testing of servers without impacting their production equivalents. The planning phase identifies what needs to be tested as part of the POC environment—base testing on your business requirements.

For example, the following steps may comprise a high-level POC plan for a single-server MOM configuration:

- Creating an isolated network for POC testing
- Installing the domain controllers
- Installing the application servers that will be monitored by MOM
- Installing the MOM server(s) (install Windows 2003 Service Pack 1 [SP1] and SQL Server 2000 SP3a or greater)
- Creating any required MOM service accounts and confirm rights to service accounts
- Installing the MOM 2005 database server and management server components
- Installing the MOM 2005 reporting components
- Creating discovery rules

- Installing MOM agents
- Installing management packs
- Configuring management packs
- Configuring notification groups and operators
- Configuring the MOM Web console and MOM web reports
- Executing tests defined for the MOM environment

The actual content of your POC plan will vary depending on your environment, but it is important to plan what steps will occur during POC. This helps you avoid a "mad scramble" of installing systems without a plan that you can leverage both in POC and in the pilot stage.

Pilot Planning

A pilot deployment moves the MOM solution that you have created into a production environment. A pilot is by its nature limited in scope. In planning your pilot you should consider how to limit either the number of servers that you will be monitoring, the number of management packs that will be deployed, or potentially both. Pilot planning should detail what servers MOM will be deployed to, what servers it will monitor, and what management packs will be utilized. Because the pilot occurs in the production environment, the production MOM hardware needs to be deployed.

Implementation Planning

The implementation phase takes the pilot configuration you created and rolls it to a full production deployment. The order in which you will add servers and management packs should be included as part of your implementation plan.

Proof of Concept

The purpose of a proof of concept is to take the design that you have created, build it, and "kick the tires." Production is *not* a proof of concept environment; When you are in a production environment you are past the proof of concept stage, and any errors you encounter have much larger costs than if you had caught them in the POC.

Setting Up a POC

Virtual Server environments make it much easier to create an isolated proof of concept environment.

A POC environment is also a great opportunity to try out a variety of management packs and see how they perform and what information they can provide. If possible, retain your POC environment even after moving on to later phases of MOM deployment. This

provides an infrastructure to test additional management packs, management pack updates, and service packs in a nonbusiness critical environment.

POC Challenges

It can be difficult to emulate a full production environment within the confines of a POC. A primary reason is hardware used in the POC environment because production-level hardware is not typically accessible. Should the type of hardware used within the POC not reflect the level of hardware in production, you may be unable to assess the speed or full functionality of your solution.

There are also some inherent challenges in any POC environment. How does one effectively scale for production? For example, if you are monitoring logon and logoff events how do you generate enough events to successfully monitor them? From our perspective, two options are available: The first is to use scripts to generate sample events that can then be run to provide a large amount of event data. The second alternative is using a *POC exclusion*, which is a document describing items that could not be effectively tested within the POC environment. This document is then used during the pilot phase to determine additional testing that needs to occur as part of the pilot.

Another complexity of POC environments is they often are isolated from the production network, removing potential interaction between the two environments. Network isolation removes the risk of inadvertently impacting production but also adds complications because production network resources are not available (file shares, patching mechanisms, and so on). If your POC testing is in an isolated environment you will want to establish a separate Internet connection to be able to patch systems and access non-POC resources.

Establishing an Effective POC

With the challenges inherent within the POC environment, how do you determine what to focus on during your POC? We suggest focusing on two major concepts: basic design validation and complexities within your specific environment.

To validate your design, test the design and determine whether there are inherent issues. This process requires deploying your design and testing MOM's basic functionality including alerts, events, notifications, and functionality using the MOM consoles. Part of basic design validation testing should also include tuning alerts and documenting your processes. If you are running in an isolated environment you will also need a domain controller, DNS, and a mail server for email notification. Basic design validation should only require a small percentage of time within your POC.

The majority of the POC time should be spent testing the complexities specific to your design or environment. For example, if your design includes Tivoli or OpenView integration this represents a complexity to test during the POC, and the other management software will need to be deployed within your POC. Although this sounds like a lot of difficulty, how would you know how the two systems will interact without any testing? The only other option is testing within the production environment, which is obviously not recommended. (Before you decide to test in production, ask yourself how your boss

would respond if your testing caused an outage in your production environment. If your boss is typical we doubt he or she would be impressed with your testing methodology.)

Other examples of potential complexities are multihomed or multitiered environments, highly redundant configurations, third-party management packs, or any requirements to create custom management packs. Your focus during POC testing should directly relate to the business requirements identified for your MOM solution.

POC testing provides a safe method to effectively assess your design and make updates as required based on results of your tests. Do not be surprised if your design changes based on the results of your POC tests.

Using POC environments also gives you the ability to configure production servers as multihomed, reporting to both production and POC management groups. Utilizing a subsection of types of production systems can provide strong insights for how MOM will function in your production environment. This gives you a method to test changes to management packs, which you can then export and import into production.

Pilot

In the pilot phase, your production hardware is deployed with MOM 2005 and integrated into your production environment but with a limited scope. In the pilot phase you are installing your production MOM hardware and implementing the architecture you designed.

Although you are deploying your production environment design, you will limit the number of servers to which the MOM agent is deployed and/or limit the number of management packs being used. The pilot phase provides a time frame to identify how various management packs respond to the production systems you are monitoring. Out-of-the-box MOM is designed to provide a limited number of alerts, but additional changes are often required to "tune" it to your particular environment. Initial tuning of MOM may occur at this point in time but is also limited in scope. During the pilot phase any POC exclusions that were identified should be tested within the actual production environment.

Tuning Rules

One of the rules you may want to tune is to adjust the amount of free space remaining in a database before MOM generates a warning. This process is discussed in Chapter 18, "Database Management." Generally, when tuning an environment the Active Directory and Exchange management packs will require the most work. This is one reason we focus on Active Directory in Chapter 16, "Managing Directory Services," and Exchange Server in Chapter 17, "Managing Microsoft Messaging."

During the pilot, track the amount of data gathered in the MOM database to determine whether your MOM database has sufficient space on a per-server basis. You can check the

amount of free space available on the OnePoint database with Microsoft's SQL Server administration tools (details are available in Chapter 18). You can also check the percentage of available free space using the MOM Operator console, in the Database Performance view using the Operational Database Free Space counter. Additionally, the TodayStatistics table in the OnePoint database provides information on the number of new alerts, new events, and other information.

Tracking MOM Database Size and Growth

Chapter 18 introduces a management pack, included with this book, that provides an automated method to track growth and space utilization for the MOM databases.

Implementation

The implementation phase moves from pilot into full production deployment. Two major methods generally are used when deploying MOM 2005 during the implementation phase: phased deployment and bulk deployment.

- Using a phased deployment approach, additional servers and management packs are added in over a period of time, allowing dedicated time for each server or management pack to tune alerts and events.

  The phased deployment approach takes a significant period of time, but you will have the benefit of thoroughly understanding each management pack and the effect it has on the servers in your environment.

- The second approach is a bulk deployment of MOM 2005, limiting notifications to the individual or group doing the MOM deployment.

  If all servers and all management packs are deployed and the notification groups are thoroughly populated, the resulting flood of alerts may annoy the recipients in the notification groups and lead them to simply ignore the alerts. The benefit of a bulk deployment with limited notification is that you can deploy the entire MOM environment quickly.

With either deployment approach, time is required for tuning MOM 2005 for your specific environment. Tuning within MOM is the process of either fixing the problems about which MOM is alerting, overriding the alerts for specific servers, or filtering the alerts.

Tuning Management Packs

Chapter 13, "Administering Management Packs," covers the basic approaches of tuning. Specific steps involved in implementing each management pack include utilizing the processes discussed in that chapter.

Maintenance

Now that you have implemented MOM 2005 you are finished, right? Not exactly. MOM is a monitoring product and will require maintenance to keep it working effectively within your environment.

Although MOM can be designed to provide responses to common error situations, MOM is intended to be monitored by operators and technical specialists. The alerts that MOM generates should be responded to and addressed. Part of regular maintenance for MOM is responding to the notifications it provides and monitoring the Operator console to respond to events and alerts that occur. The tasks included within the various management packs are designed to provide an efficient manner to perform common maintenance tasks.

Like other systems, your MOM server environment will require maintenance through deployments of software patches, service packs, antivirus updates, backups, and other regularly scheduled maintenance such as the MOMx grooming SQL Server job (which we discuss in Chapter 10), and the database maintenance jobs created as part of the MOM database setup.

Another part of the maintenance phase is maintaining management packs within MOM. Management packs constantly change. Existing management packs are updated by Microsoft as new features or bug-fixes are identified. New management packs are created by Microsoft, third-party vendors, and other MOM administrators providing management packs available for download from the Internet. As part of the maintenance phase you need to consider additions, updates, or removal of management packs.

Agents in MOM also require maintenance. As new servers are added to your environment, MOM agents should be deployed to monitor them. Likewise, as older servers become obsolete and are replaced their agents should be uninstalled. Agent software will also require updates as service packs are applied to the management server.

In summary, within the maintenance phase it is important to monitor, maintain, and update your MOM infrastructure. MOM environments are constantly evolving because the infrastructures that they support are continually changing.

Sample Designs

This chapter contains a lot of guidance and information, and it can be a bit overwhelming to absorb and translate to a design. However, many MOM implementations fit into the same general guidelines. Taking a closer look at a sample organization and how its MOM environment is designed can give some clues into your own organization's design.

We will look at three sample designs to get an idea of how the process works.

Single Server MOM Design

Coyote is a 300-user corporation that operates out of its headquarters in San Francisco. A single Windows 2003 domain, coyote.com, is set up and configured across the enterprise.

In company headquarters, 30 Windows Server 2003 servers operate as file servers, DHCP servers, DNS servers, SQL 2000 database servers, and Exchange 2003 messaging servers.

Because of a recent spate of system failures and subsequent downtime, which could have been prevented through better systems management, Coyote's IT group looked at MOM 2005 to provide much-needed systems management for its server environment.

Because the amount of servers to be monitored was not greater than 100, Coyote decided to deploy a simple management group consisting of a single MOM server running all MOM components. The server chosen was a dual-processor P4 2.4 GHz server with 2GB of RAM and redundant hardware options.

A single management group was created for all servers, and the MOM 2005 agents were distributed throughout the server infrastructure. In addition, the default management packs were deployed and configured for the Base OS, DNS, DHCP, Active Directory, Exchange, and SQL Server.

Figure 4.10 shows the final design.

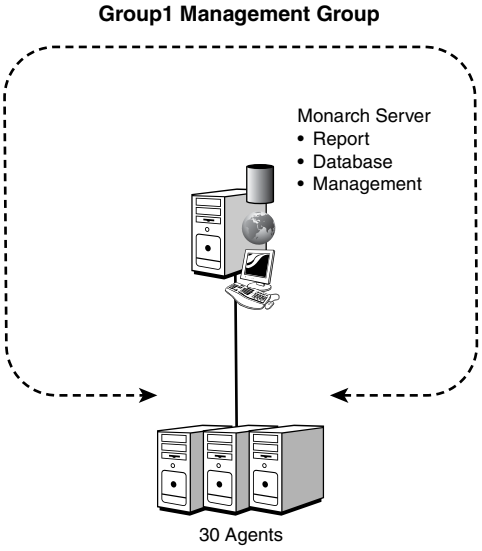


FIGURE 4.10 Coyote single server design.

Coyote's MOM administrator feels that the company can easily scale its MOM implementation to higher numbers of servers if it wants because the hardware can accommodate increased numbers of users. Coyote is mildly concerned with the single point of failure that the single MOM server has but decided that it is more cost effective for the organization to deploy a simple single-server management group.

Table 4.21 summarizes the design points and decisions.

TABLE 4.21 Coyote Single-Server MOM Design Summary

Design Point	Decision
Monitored computers	30
Management group	1
Management group name(s)	Group1
MOM server(s)	1
Operations database retention	4 days
Estimated operations database size	1GB
Reporting database retention	1 year
Estimated reporting database size	100GB

Single Management Group Design

After using MOM 2005 for a period of time, Coyote decides it needs redundancy and better performance for MOM. The company also goes through a round of acquisitions, which increases the number of managed computers to a total of 500 servers.

Coyote wanted to retain its operations data for a year, which referring back to Table 4.20 would be under 1TB of storage. It also evaluated the operations database retention and decided that the default of four days is sufficient, which would result in an operations database size of 10GB per Table 4.19.

The design chosen was a single MOM management group named Group1 with a classic four-server design including a database server (Fountain), a reporting server (Silverthorne), and two management servers (Monarch and Keystone). The servers chosen were all dual-processor P4 2.4 GHz servers with 2GB of RAM and redundant hardware options. Figure 4.11 shows the diagram.

For the storage requirements, the database server used a dual-channel controller with a mirrored set of 72GB drives for the OS/logs and a RAID5 set of three 72GB drives for the database. The reporting server used a dual-channel controller with a mirrored set of 72GB drives for the OS/logs and an external array with a total capacity of 2TB.

The dual-management server configuration allowed Coyote to assign 250 of its managed computers to each of the management servers. In the event of a failover, either management server could handle the load of 500 total agents. This gives Coyote the fault tolerance needed.

In the event of a database server outage, the management servers and agents will buffer the operations data. The data center stocks standard spare parts and servers to be able to restore operations within four hours. The reporting server will take longer to bring back to full operations, but this is considered less mission-critical because the only impact will be report generation capabilities.

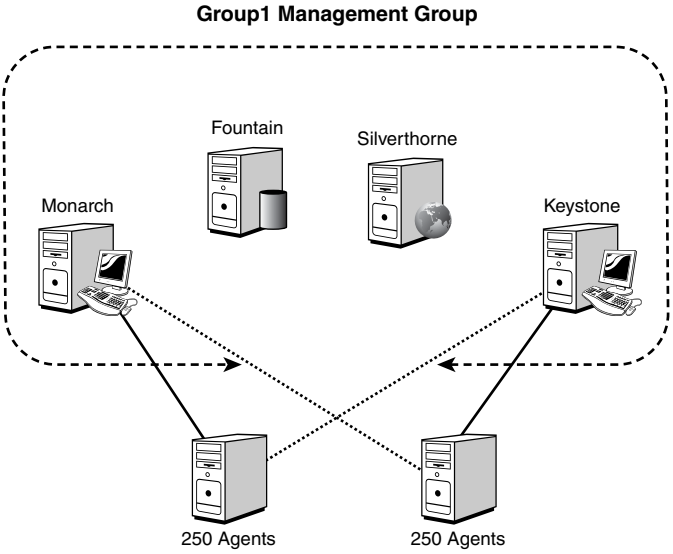


FIGURE 4.11 Coyote multiserver design.

Table 4.22 summarizes the design points and decisions.

TABLE 4.22 Coyote Single Management Group MOM Design Summary

Design Point	Decision
Monitored computers	500
Management group	1
Management group name(s)	Group1
MOM server(s)	4
Operations database retention	4 days
Estimated operations database size	10GB
Reporting database retention	1 year
Estimated reporting database size	100TB

Multiple Management Group Design

Contoso is a large, 5,000-user corporation with three major offices in New York, London, and Tokyo. Each major location currently hosts between 100 and 150 servers. Most of the servers are Windows Server 2003 machines, but a minority is composed of Novell NetWare, Linux, and Windows 2000 machines. Contoso utilizes a Windows 2003 Active Directory forest composed of a subdomain for each region, as shown in Figure 4.12. In the North America region New York resides in the na.contoso.com domain; in the European region London resides in the eu.contoso.com domain; and in the Asia-Pacific region Tokyo resides in the ap.contoso.com domain. Each domain is part of the same Windows 2000 forest under the root contoso.com domain, as shown in Figure 4.12.

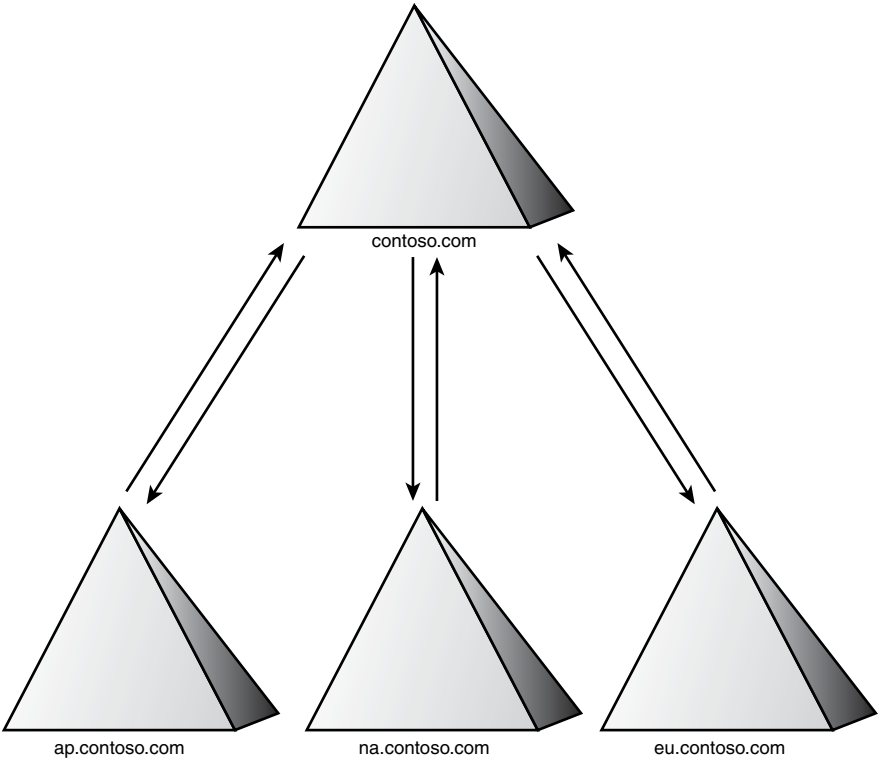


FIGURE 4.12 Contoso forest.

Contoso needs to deploy a robust server management system to increase its uptime levels and improve productivity across the enterprise. It chose MOM 2005 to accomplish this task.

The early design sessions indicated that three management groups for MOM would be required, one for each geographical location. This is due to the independent nature of the three regions. MOM-to-MOM product connectors would be set up between the management groups and a global management group to allow for alerts to be rolled up to the global management group. Figure 4.13 shows the design.

Each of the regional management groups would manage up to 150 servers, so a single server was deployed with both the database and reporting components. Two management servers were deployed for each regional management group, with the MOM Connector Framework (MCF) and the connector to the global management group on one of the management servers. Given the 150 managed computers, the total storage needed was approximately 250GB for the reporting database. For the storage requirements, the combined database and reporting server used a dual-channel controller with a mirrored set of 72GB drives for the OS/logs and a RAID5 set of eight 72GB drives for the databases. The total storage for the databases was approximately 500GB.

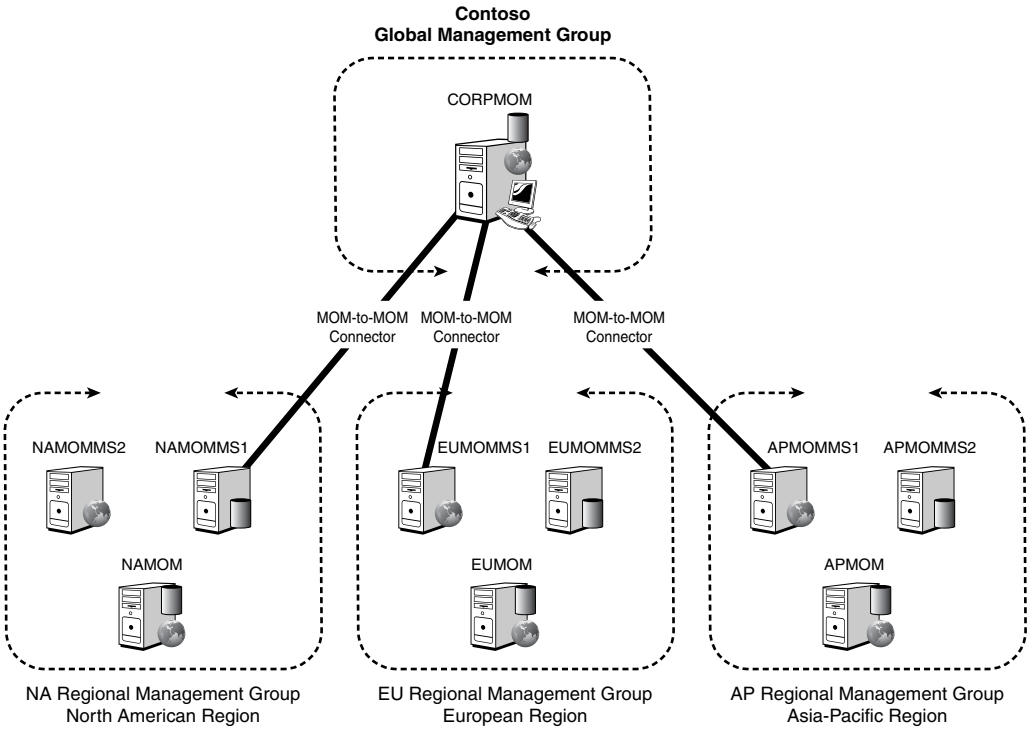


FIGURE 4.13 Multi-management group design.

The global management group consists of a single MOM server with all the roles. The main purpose of the global management group was to provide a single pane of glass to see all the alerts for all regions. Given that, it is not considered a mission-critical function, and redundancy was not needed. The storage requirements were minimal because it would not be supporting any agents directly.

Contoso made extensive use of the Microsoft management packs and purchased add-on management packs from third-party vendors to manage its disparate operating systems and application environments.

This design allows the organization to have a corporate view of all alerts within the entire company but still allows the regions to have full operation control over their servers and utilize the MOM 2005 features to ensure uptime. The strategic placement of roles allows for server consolidation and redundancy where needed.

Table 4.23 summarizes the design points and decisions.

TABLE 4.23 Coyote Single-Server MOM Design Summary

Design Point	Decision
Monitored computers	450
Management groups	4
Management group name(s)	Contoso
	NA
	EU
	AP
MOM server(s)	10
Operations database retention	4 days
Estimated operations database size	3GB (each region)
Reporting database retention	1 year
Estimated reporting database size	300GB (each region)

Summary

This chapter explained why it is important to develop a plan before implementing MOM into your environment. We discussed assessment and design as a part of that plan, as well as some of the technical design considerations for the various components of a MOM infrastructure. We also discussed the planning phases needed to effectively deploy MOM 2005 into your organization and looked at some sample designs. The next chapter discusses planning complex MOM 2005 configurations.

CHAPTER 5

Planning Complex Configurations

IN THIS CHAPTER

- Planning for Redundancy
- Planning a Multitiered Deployment
- Planning a Multihomed Deployment
- Planning for Multiple Domains
- Connecting MOM

This chapter discusses how to go about planning more complex configurations of Microsoft Operations Manager (MOM). By "complex," we mean either achieving fault-tolerant systems by implementing redundant management servers and clustered database servers and/or allowing multiple management groups to communicate with each other or with other management systems.

As part of planning complex configurations with MOM 2005, remember the assessment, design, planning, proof of concept (POC), pilot, implementation, and maintenance stages. These were introduced in Chapter 4, "Planning Your MOM Deployment," and should be used when planning your MOM implementation.

Planning for Redundancy

MOM is designed to provide a stable monitoring solution that can function effectively even if one server malfunctions. It is up to you as to what redundancy features to implement. Redundancy requirements should be identified during the assessment phase of your MOM 2005 deployment. Various components within MOM can be designed to provide a redundant configuration: These include management servers, database servers, reporting servers, and reporting database servers.

From a planning perspective, redundancy requirements should be identified during the assessment stage. Document details of the redundancy within the design phase—including how many management servers will be installed, where they will be located, and the agents for

which they will provide primary and failover monitoring. MOM 2005 supports a clustered OnePoint database and a maximum of 10 management servers in a single management group (we will discuss clustering the MOM database in the "Database Servers" section of this chapter).

During your proof of concept, you should install a representative sample of management servers to test how agents will respond to loss of communication to both primary and failover servers.

Management Server Redundancy

A common practice is having at least two management servers in your primary location (where the OnePoint database typically resides) and split agents between those two management servers. This will provide both load balancing between the servers and redundancy.

During the pilot stage, the redundant server configuration is deployed, and redundancy functionality should again be tested. Within the implementation stage all management servers are deployed in accordance with your design.

Impact of Failures

MOM includes a certain amount of built-in redundancy to its components. Knowing the limits of this redundancy will help to define the placement of MOM components in your design.

MOM management servers are by definition, redundant components. If an agent uses a particular management server, and that server experiences a hardware problem, another management server will take over the management server role for that agent. Consequently, having at least two management servers may be warranted if your desire is to provide a high level of uptime for your MOM environment.

The MOM database is a single point of failure for a MOM management group, making it important to establish a robust fault-tolerance scheme for this server because there is no built-in redundancy for this server. Use of a SQL replication or SQL clustering solution may be possible to help mitigate potential redundancy concerns with the database, as discussed later in the "Database Servers" section of this chapter. And of course, backups are of paramount importance.

One of the important aspects of the design is what happens when there is a breakdown in communication between components. Table 5.1 summarizes the impacts of communications problems between various MOM components.

TABLE 5.1 Impacts of Communication Failure

Failure	Impact
Agent to management server	In the event that the agent cannot communicate with the management server, the agent will attempt to contact backup management servers and continue normal operations. If the agent cannot contact another management server, it will then buffer the data until the local storage limit is reached (which is a defined configuration setting). Local actions continue to take place as cached rules dictate. When the management server becomes available, the agent will send data and will also send a heartbeat failure alert. At the same time, the management server will have detected that the agent is not heartbeating and will attempt to contact the agent using a ping. It then reports the availability of the agent and the managed computer. After the agent reconnects, the management server will generate a success event.
Management server to database server	If the management server loses its connection to the database server, the management server will buffer the data coming from the agents it manages. If the buffer fills, the management server will stop taking data from agents until it reconnects with the database. After the connection with the database is established, the management server will upload the buffered information and resume accepting data from its agents.
Database server to reporting server	If the DTS process that transfers information from the operations database to the reporting database fails, the process is tried again at the next interval (default is daily). The data that has not been transferred from the operations database to the reporting database will not be groomed until either the DTS transfer process is successful or 60 days have passed with no successful transfer. At that point the data at the 60-day mark will start to be overwritten.
Management group to management group	The MOM Connector Framework (MCF) forms the basis of the MOM-to-MOM Connector, which connects management groups via management servers. If the management servers cannot connect, they will stop forwarding alerts and updates, but all other management group functions continue normally. Alerts will be forwarded when the management servers reconnect.

Management Servers

As discussed in Chapter 4, management servers provide communication between monitored systems and the MOM database. Unlike the MOM database servers, management servers are not supported on a clustered platform because redundancy is provided via the failover capabilities of the management servers. Deploying multiple management servers is one of the most common approaches used when implementing failover in a MOM environment. Multiple management servers are often utilized in mid-sized organizations without redundant database servers, due to the additional costs in hardware and software licensing associated with database clustering. However, you should note that redundancy for both the management servers and database servers is required to provide a fully redundant MOM solution. From the management server perspective, redundancy can be achieved by installing multiple management servers within a single management group. When an agent's primary management server is unavailable, it will send its data to its failover management server.

The management servers can be configured to fail over in a specific pattern to ensure that no one management server receives the entire load. Figure 5.1 shows the agents' primary management server with a solid line and then the failover order for each group of agents using a dashed line with a number. The number represents the failover order. For example, the A group of agents would fail over from MS1 to MS2, then to MS3, and finally to MS4.

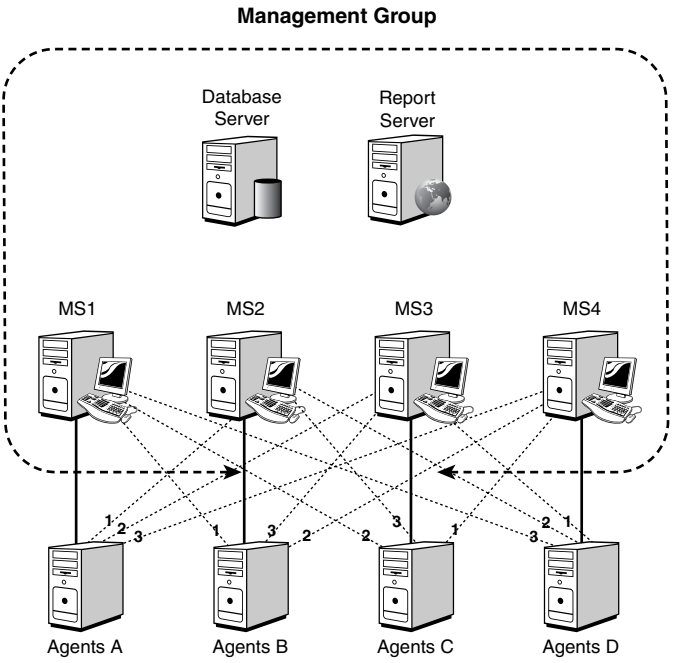


FIGURE 5.1 Balanced agent failover diagram.

The failover order is configured on each management server and applies to the agents for which it is the primary management server. In the case of management server MS1, it is the primary for the A group of agents. Table 5.2 shows the configuration that you would set for each management server.

TABLE 5.2 Balanced Agent Failover Configuration

Management Server	MS1	MS2	MS3	MS4
MS1		1	2	3
MS2	1		3	2
MS3	2	3		1
MS4	3	2	1	

Agent Internal Settings

The information related to what agent primary and failover management servers and the communication port (TCP/UDP 1270 by default) can be seen in the registry on the monitored system in the HKLM\SOFTWARE\Mission Critical Software\OnePoint\Configurations\<*management group name*>\Operations\Agent\Consolidators key:

- String values exist for "Consolidator 1 AD Name," "Consolidator 1 Host," and "Consolidator 1 Secure Port."
- Each instance of a failover server increases the numbers, so for example these would be "Consolidator 2 AD Name" and "Consolidator 2 Host."

For example, Contoso also has a Dallas location with two management servers: Monarch and Keystone. These two servers support 500 servers and have the load split evenly between them (Monarch is the primary management server for 250 servers and failover for 250 others; Keystone is primary for 250 servers and failover for 250 servers). SQL Server Reporting Services is installed on the Silverthorne server, and the Lakewood server houses the MOM reporting database. The DAS components running on the management servers (Monarch or Keystone) communicate with the MOM database (Fountain) via OLEDB. By default this traffic is not encrypted, but you can use Internet Protocol Security (IPSec) or OLEDB Encryption (Secure Sockets Layer or SSL) for a secure connection. The "Reporting Servers and Database Reporting Servers" section later in this chapter discusses redundancy for the database components.

Figure 5.2 shows the Contoso MOM 2005 configuration for the Contoso_Admin management group.

Database Servers

Although implementing redundant management servers provides a first step in designing a redundant MOM configuration, we also need to consider the operational data store. If the MOM database server fails, MOM cannot store the operational information sent to the management server; so fault-tolerant configurations should also consider database

server redundancy to provide a truly redundant MOM solution. If the MOM database server is not functioning, the management server(s) will queue data while the database is offline, but the queue eventually fills and data will be lost. Also, the consoles cannot display data when the MOM database is offline. Implementing a separate database server from the management server splits the load between the systems and allows you to implement technologies such as server clustering, which provides MOM database server redundancy.

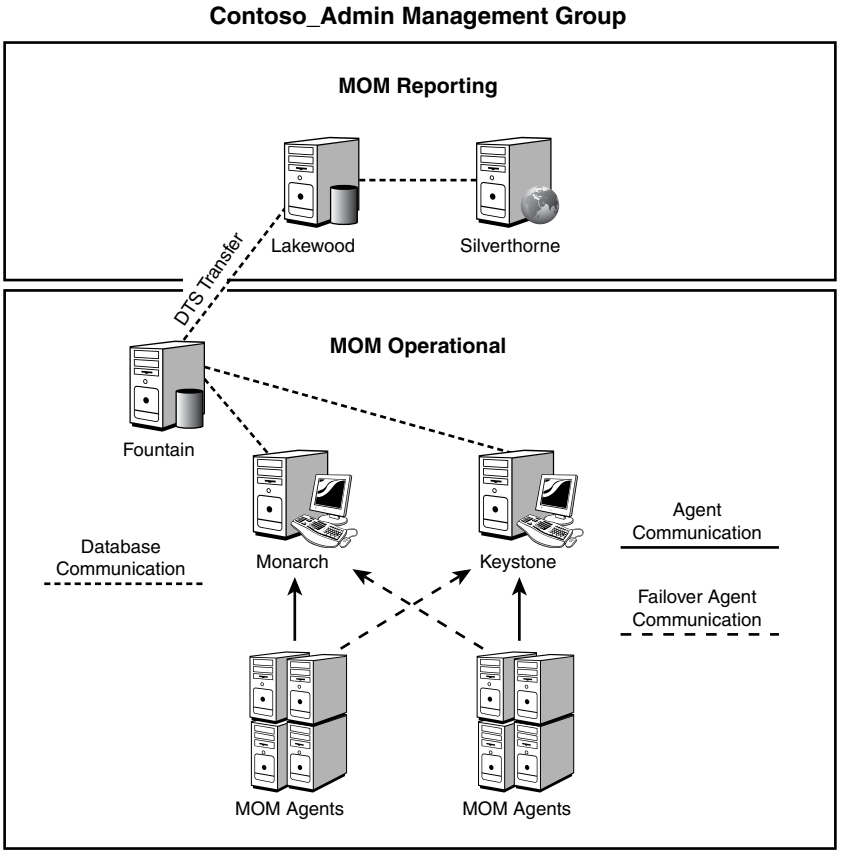


FIGURE 5.2 Redundant management servers.

Clustering technologies connect two or more servers to a shared source of data. In a clustered implementation, if one of the cluster members fails another takes over for the failed system. Microsoft SQL Server supports database clustering, and MOM 2005 supports implementing a clustered MOM database server.

Server clustering requires additional hardware and software purchases that can make it an expensive solution for redundancy. Implementing clustering requires specific operating systems listed in Table 5.3 and versions of SQL Server shown in Table 5.4.

TABLE 5.3 Operating System Editions and Server Cluster Nodes

Operating System	Edition	Cluster Nodes
Windows 2000	Advanced Server	2
Windows 2000	Datacenter Server	4
Windows Server 2003	Enterprise Edition	8
Windows Server 2003	Datacenter Server	8

TABLE 5.4 SQL Server Editions and Cluster Nodes

SQL Server	Edition	Cluster Nodes
2000	Advanced Server	2
2000	Datacenter Server	4
2005	Enterprise Edition	4
2005	Datacenter Server	8

From a hardware perspective, at least two servers are required that are connected with a shared data array. All the hardware, including the external array, needs to be on the Hardware Compatibility List Cluster Solutions (available at http://www.microsoft.com/windows/catalog/server/default-v1.aspx; click on the Hardware tab and then browse the hardware cluster solutions). More details on recommended database concepts including RAID configurations are discussed in Chapter 10, "Complex and High Performance Configurations."

Although the cost of a redundant MOM database server may seem high, clustering provides a redundant configuration for the database. You can also take advantage of a clustered configuration to apply software patches and updates without incurring downtime and production outages.

For example, after a recent monitoring outage our fictitious company Contoso decided it needed a redundant database server configuration in addition to its redundant management server configuration. To meet this requirement Contoso implemented changes to its environment (shown in Figure 5.3), replacing the original database server (Fountain) with a database cluster called Evergreen.

SQL Server Primer: Failover Mechanisms

Although database backups and clustering the SQL database are the only supported backup/failover mechanisms for MOM 2005, SQL Server itself does provide several other options for database recovery. These alternatives are log shipping and database mirroring:

- Log shipping is a manual procedure used with SQL Server 2000 Enterprise Edition that applies the transaction logs from the primary server to a secondary database server. It requires that the Full recovery model be configured for any databases that you will be log shipping.
- Database mirroring, available with SQL Server 2005, has similarities to the log shipping feature in SQL Server 2000. Entries from a transaction log in one

database are transferred and applied from its instance on a primary (now known as "principal") to its copy on a secondary server (known as the "mirror" server). Like log shipping, mirroring requires the principal database to be in Full recovery mode. The process can be automated with a third instance of SQL Server 2005, although this capability is not available using SQL Server 2005 Express Edition. Note that the default and recommended recovery configuration for both the operational and reporting MOM 2005 databases is Simple mode, which does not write transactions to the transaction log.

Because the MOM databases use the simple recovery option, clustering is recommended to provide automated recovery in the event of a MOM database server failure and is the approach we will follow when discussing database redundancy.

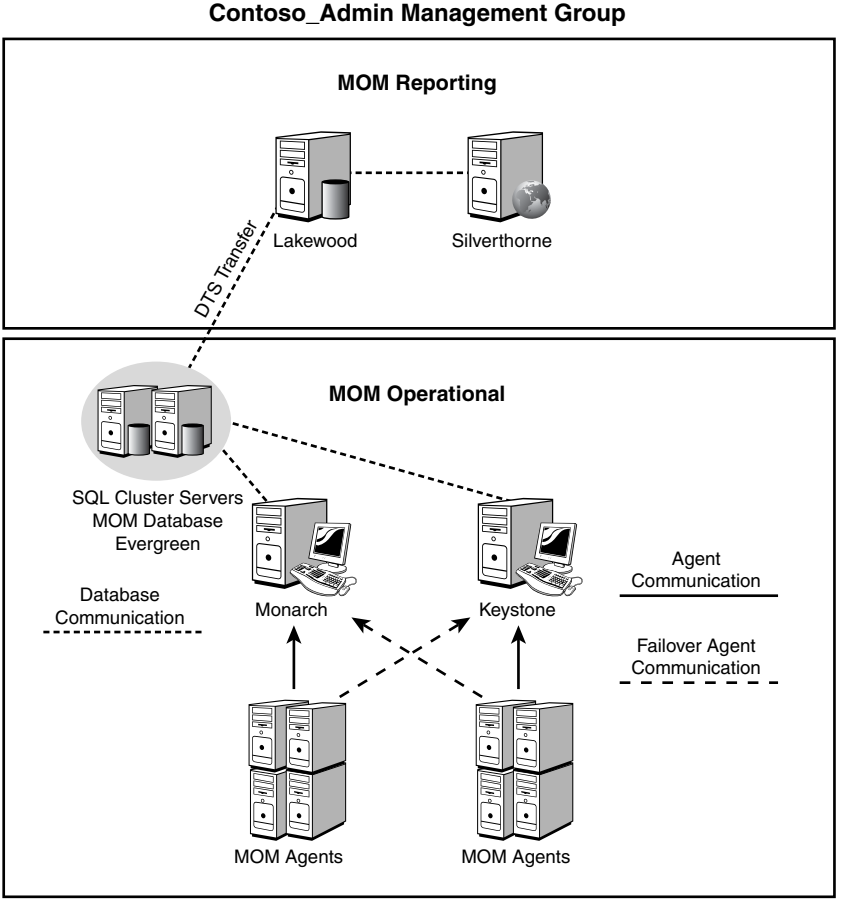


FIGURE 5.3 Redundant management servers and databases.

Reporting Servers and Reporting Database Servers

For most organizations, having a redundant management server and database server configuration will provide as much redundancy as necessary. Redundancy for the reporting servers and/or reporting database server is not a common requirement. However, if the reports MOM produces are also business critical (and must be highly available) you can design a fully redundant MOM 2005 reporting configuration as well.

Servers providing reporting functionality for MOM 2005 utilize SQL Server Reporting Services, which provides the web-based reporting used with MOM 2005. Management packs written for MOM 2005 include reports that work with SQL Server Reporting Services (SSRS), using information from the MOM reporting database and presenting it within a web interface. The SSRS application can run on the MOM reporting database server or be installed on another server.

Redundancy with Network Load Balancing

If you separate SSRS to an additional server, redundancy for the reports within SSRS can be met by implementing Network Load Balancing (NLB) on the servers. An NLB *cluster* uses multiple servers, so if one reporting server is unavailable, another server provides the reporting service, transparent to the user.

NLB is available with Windows 2000 Advanced Server, Windows 2000 Datacenter Server, or any version of Windows 2003 (Windows 2000 versions require a minimum of Service Pack 2). The load balancing capability of NLB allows the network load to be efficiently spread across multiple servers, increasing the scalability of applications such as high-volume websites and proxy services.

NLB works by creating a virtual adapter that represents all the servers in the actual NLB cluster. Hardware requirements for NLB are minimal (one additional network adapter per server is recommended to provide a "heartbeat" between the systems). NLB does not currently have the functionality to remove inactive servers from the cluster; this can be accomplished by using third-party load balancing appliances.

Redundancy with Clustering

As with the MOM production database servers, the MOM reporting database servers used with the SSRS component can also be designed in a redundant configuration by using database clustering.

Supported Clustered Configurations Prior to Service Pack 1

MOM 2005 without Service Pack 1 does not support Active/Active clustering of its databases. A passive node is required, so the Active/Passive and Active/Active/Passive configurations are supported. No more than one instance of the MOM database can be running per instance on the cluster, but other applications can run in Active/Active mode on the same cluster as the MOM database if necessary. MOM 2005 also does not support a cluster where one node runs the OnePoint database and the other node runs the MOM reporting database.

If you attempt to install the Reporting component on an Active/Active cluster that runs on the MOM database, you may receive an error of "unable to determine Microsoft

Operations Manager Database version." If you encounter this error and you want to run the MOM 2005 reporting database on the Active/Active cluster, you can use the Regedit utility (regedit.exe) to create the following key: HKLM\SOFTWARE\Microsoft\Microsoft Operations Manager\2.0\Setup\InstalledServerSKU as type Reg_SZ with a value of Select. This allows you to continue the reporting database component installation.

One morning the Contoso CIO was unable to access his daily operations reports. Soon after, the company determined that all MOM 2005 components were critical to its business function and required full redundancy. To meet this requirement the Lakewood and Silverthorne servers were replaced by the Ridgeway cluster for MOM Reporting and a network load-balanced configuration (Breckenridge) was built for housing SSRS, as illustrated in Figure 5.4. This configuration provides full redundancy for Contoso for all components in its MOM 2005 implementation.

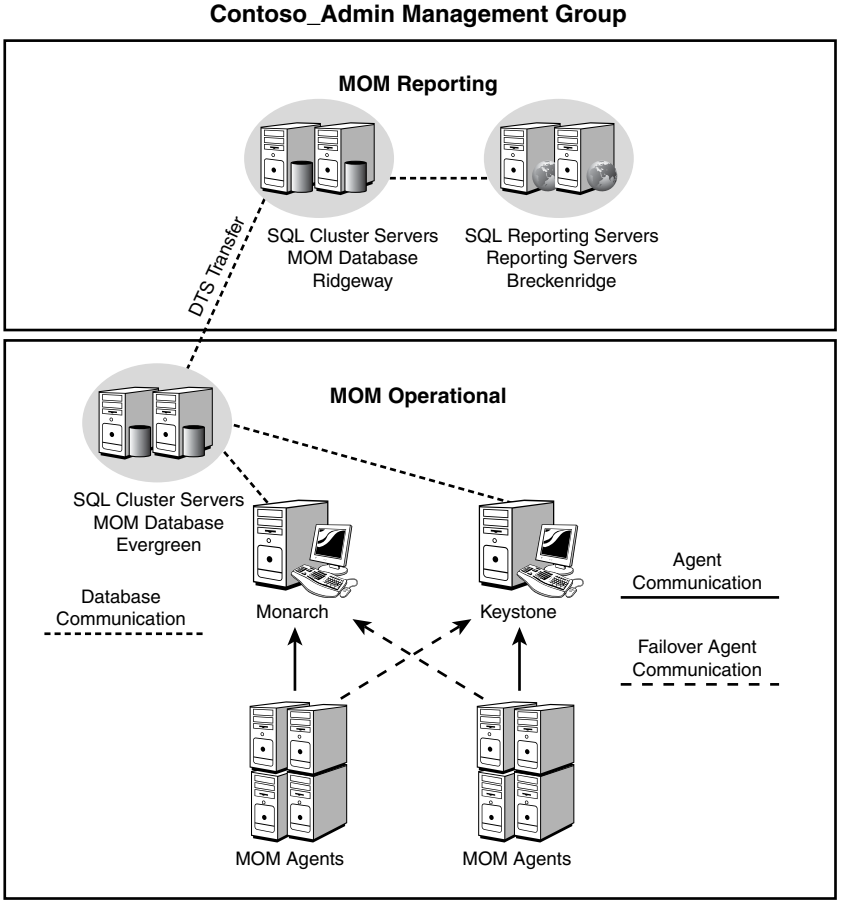


FIGURE 5.4 Fully redundant MOM configuration.

Redundancy Without Clustering

Another option that provides a higher level of redundancy than a single server configuration is using SQL Server replication to copy data to another database. For example, we could replicate the data from the Lakewood database server to the Evergreen database cluster (or to another database server). In that configuration we can reconfigure SQL Server Reporting Services (Silverthorne) to use the replicated copy of the data.

To provide redundancy for SQL Server Reporting Services we could also install SSRS on the Lakewood database server so that the server includes both the OnePoint and SystemCenterReporting databases. This configuration removes a single point of failure: Should the Lakewood database and reporting server fail, the Evergreen cluster also contains a copy of the data, which can be made accessible from the Silverthorne server. If the Silverthorne server fails, the database on Lakewood could be accessed directly to provide the reports. Figure 5.5 illustrates an example of this configuration.

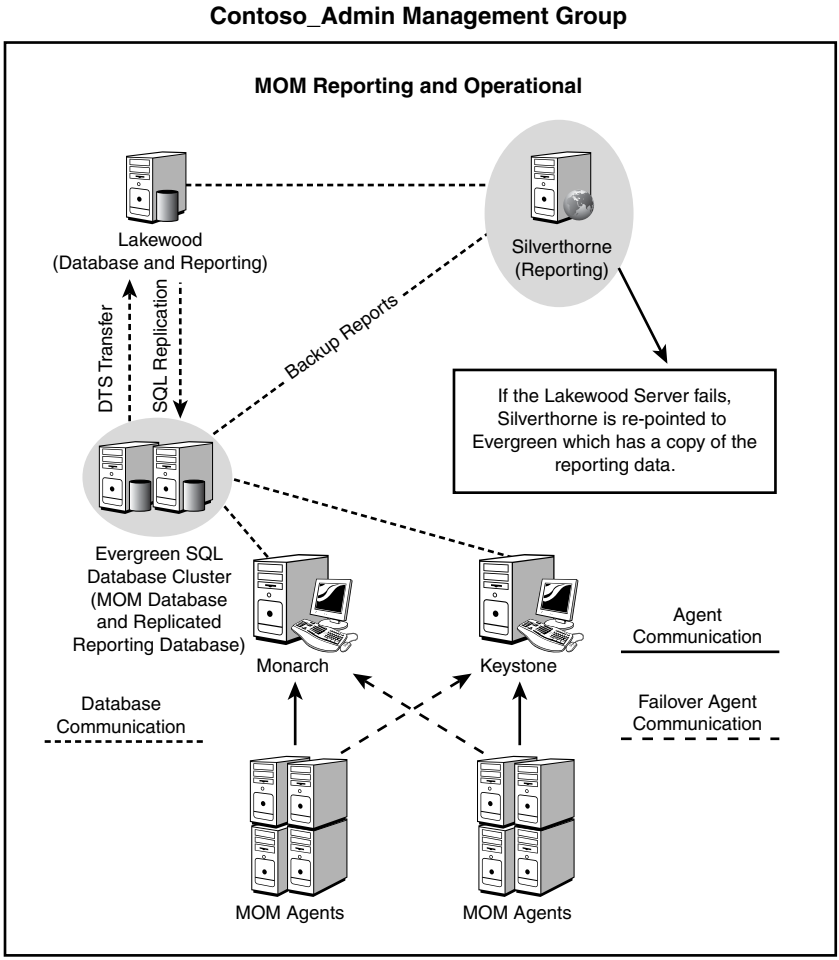


FIGURE 5.5 Alternate redundant MOM configuration.

Re-Pointing SQL Server Reporting Services

A SQL Server Reporting Services system can be re-pointed to a different database server by changing the SCDW configuration. To do this, browse to the reports website (in our example http://silverthorne/reports) and click on SCDW. Change the ConnectionString field to reference the new location (in our example evergreen\sqlcluster).

Planning a Multitiered Deployment

One of the complex MOM deployment solutions utilizes multiple management groups, where one or more management groups report information to a higher level management group. A multitiered design such as this must be properly planned for effective design and implementation.

Structuring Multiple Management Groups

Within the assessment phase, business requirements can lead to the design of a multitiered design, as discussed in Chapter 4. Examples include exceeding supported management group scale limits, separating administrative control, and multiple physical locations with large numbers of servers. Regardless of why a multitiered approach is required, it needs to be planned as part of the deployment.

Common approaches to split management groups include splitting the managed computers geographically or by departments. As you design your management group solution, consider connecting your management groups using the MOM Connector Framework (MCF) and the MOM-to-MOM Product Connector (MMPC).

MOM-to-MOM Product Connector

What is the MOM-to-MOM Product Connector (MMPC)? The MMPC is a technology designed to connect two different MOM management groups.

The MMPC uses the MOM Connector Framework, a web service written in .NET managed code, to send information between two MOM management groups (source and destination groups). The MMPC synchronizes the alerts between the two management groups. The MMPC is a Microsoft Windows service running on the management server that uses the DAS account to access the database on the source management group. It also uses the Internet Information Server (IIS) World Wide Web service on the destination management group.

Structuring a Multitiered Hierarchy

A MOM *hierarchy* exists when one or more management groups report information to a higher level management group. Establishing a hierarchy provides a view of your entire business and a single location for managing alerts, allowing you to monitor the entire enterprise from a single MOM Operator console.

For example, Figure 5.6 shows a common scenario of a two-tiered management server implementation for a global corporation, with server operations in North America, Europe, and Asia-Pacific regions.

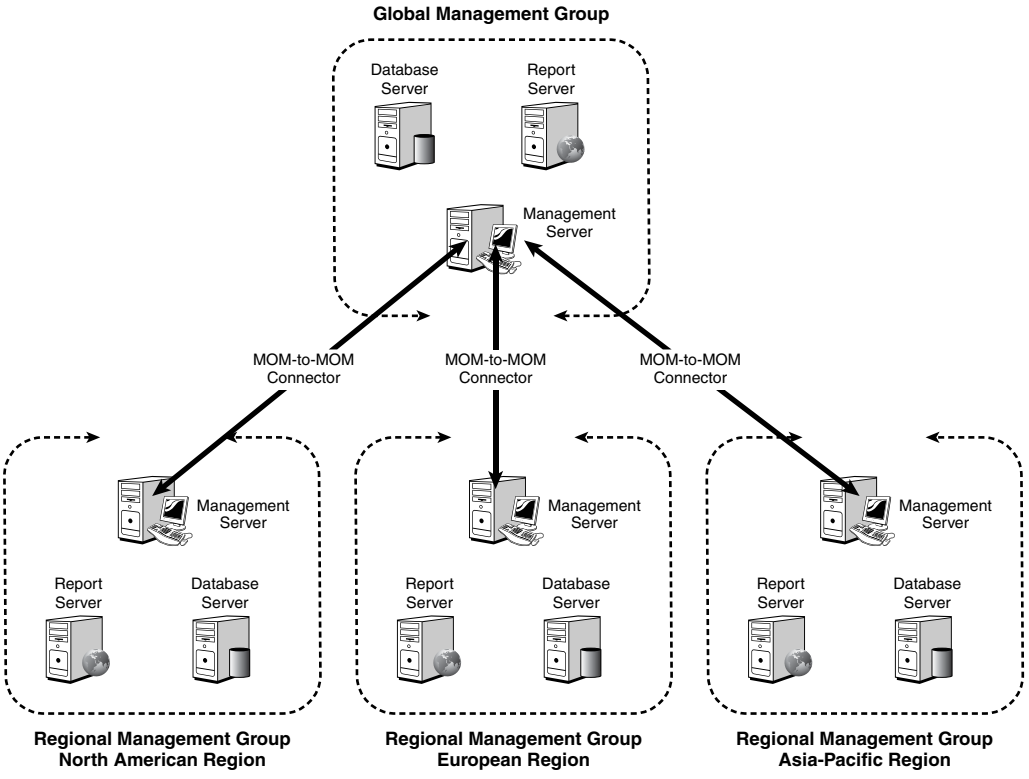


FIGURE 5.6 Two-tiered management group implementation.

Architecturally, management groups can be integrated at the alert level using the MOM-to-MOM Product Connector. We discuss implementing the MMPC to connect multiple management groups in Chapter 19, "Interoperability." Using the connector, management groups can be configured to forward alerts and some discovery data bidirectionally to a master management group. Other data types, such as performance or event data, are not integrated between management groups. Figure 5.6 shows an enterprise deployment with three regional management groups forwarding their alerts to the global management group. Once forwarded, the alerts would be bidirectionally synchronized, meaning that as changes are made to the alert at either the global operations console or the regional operations console they would be propagated across the link.

For example, say that a forwarded alert issue is resolved by the global Information Technology (IT) staff. The global IT staff updates the alert as resolved, and the history is also updated at the global MOM 2005 management server. The alert is then automatically resolved and the history appended at the regional MOM 2005 copy of the alert. On the flip side, if the regional IT resolves the issue and updates the alert in its regional MOM 2005 Operator console, the changes are immediately propagated up to the global MOM 2005 Operator console. Both the regional and global IT stay completely up-to-date with the alert as it is handled and resolved.

Within the proof of concept stage, you should replicate the management group configuration you designed (in the case of very large configurations, you can use a subset of your management groups). During the POC, the focus of testing multiple management groups should be on how they are communicating with the MCF and MMPC.

Planning a Multihomed Deployment

Another configuration with added complexity is the multihomed configuration. In a multihomed configuration a single server's agent belongs to more than one management group. A good question might be: "Why have an agent report to more than one management group?" There are several good reasons for having an agent report to multiple management groups, including

- **Separation of functions**—Within some organizations, different groups manage different functions such as the operating system platform, messaging, and database. Each group might have its own MOM 2005 management group with the appropriate rules and operators. The agent on any given server would report to the appropriate functional management groups.
- **Security**—As the IT industry has matured and grown, the security requirements have matured and grown as well. Many organizations are bound by regulatory requirements for the security department to collect security and audit information in an independent manner and with long retention periods. MOM 2005 allows the security department to have a security management group separate from the organization's operations management group. The security department would have exclusive control and access to the security management group, deploying the appropriate rules and with the appropriate retention levels. This management group would leverage the existing MOM agent deployed by the operations management group.
- **Scale**—As organizations grow and become more distributed, the central office frequently cedes more and more operational control to the regional offices. However, the central office may still require a measure of control over branch office servers. MOM 2005 allows the organization to scale by allowing the regional servers

to be managed by regional management groups but also have the regional servers' agents report to the central office management group. The central office would typically deploy a limited set of rules, rather than the whole assortment of rules that deploy by default.

A multihomed configuration is not uncommon and is often used for a MOM agent to report to a security-only management group as well as a nonsecurity management group. This provides an example of when to create a multihomed deployment to meet two of the criteria listed previously: separation of functions and security.

Recently Contoso created a new security division. This new security division requires the capability to gather security information from all servers, and all rules it uses must only be alterable by the members of the security division. To meet this new requirement Contoso added a second management group and made the agents multihomed, as shown in Figure 5.7. The security division does not require reports, removing a requirement to either deploy a reporting solution for the security division's management group or integrate both management groups into a single reporting environment using the Multiple Management Group Solution Accelerator (the MOM Solution Accelerators are discussed in Chapter 19), which aggregates data from multiple management groups into a central data warehouse for consolidation and reporting.

Each management group has its own OnePoint database. The Contoso_Admin management group manages all aspects of servers except for security, whereas the Contoso_Security management group manages the security information for all servers. MOM 2005 allows each management group to work independently of the other. For example, if the Contoso_Security group generates an alert to notify administrators if security log event 517 occurs (the audit log was cleared), the Contoso_Admin group collects the event but does not generate an alert. The specific rules used enable the MOM agent to determine which response (or lack of a response) to provide to each management group.

A requirement for a multihomed configuration should be identified during your assessment stage. The necessary management groups should be designed in the design stage and tested in the POC phase. As with other complex MOM deployments, a multihomed configuration should be a focus during both the POC and pilot phases. POC testing should include items such as how the agent responds to loss of one or more of the management servers that it belongs to, and results of different responses to the same data going to different management servers.

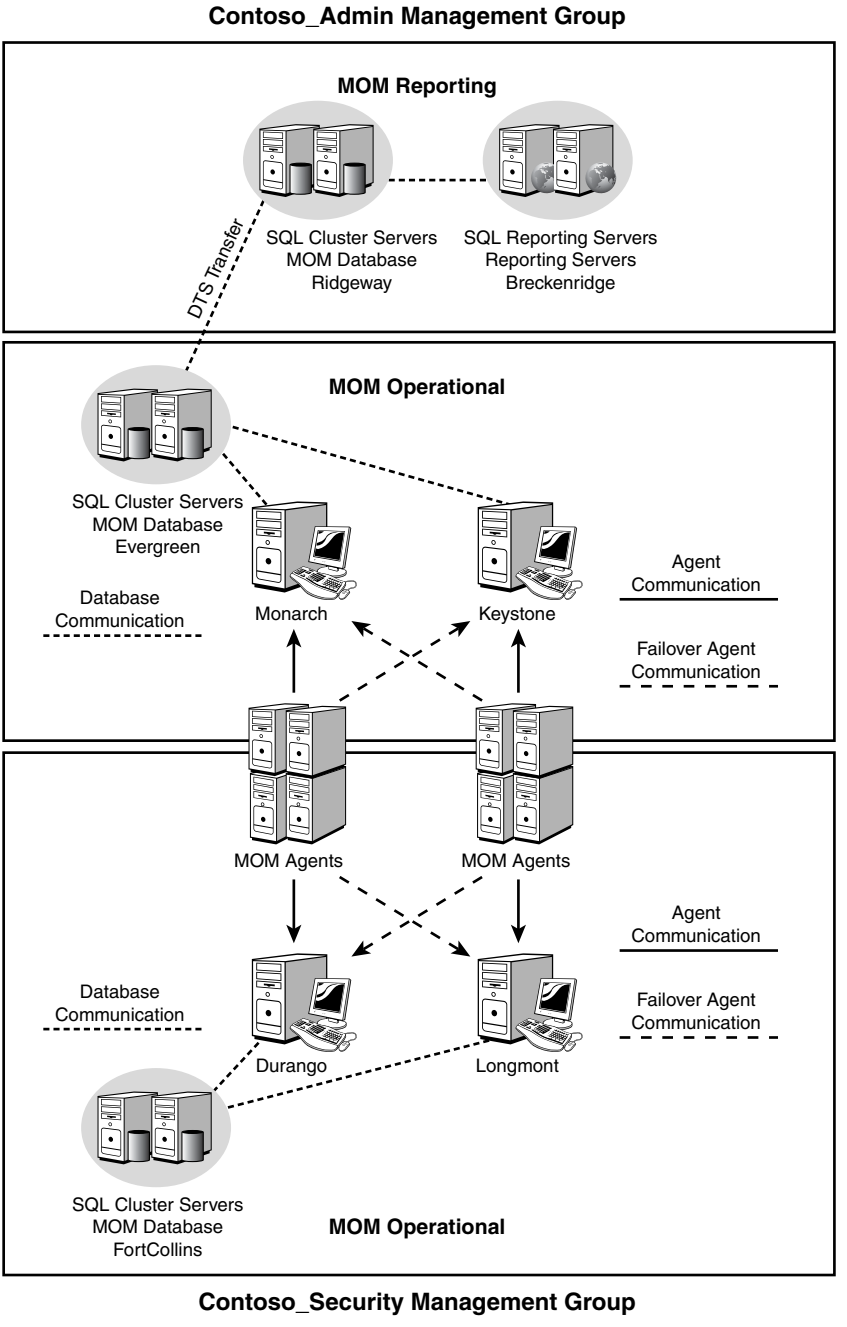


FIGURE 5.7 Multihomed MOM configuration.

Planning for Multiple Domains

When planning MOM 2005 in a multiple domain configuration there is one major concept to remember: Agents deployed to target computers must use credentials that have rights to the domain the agent is being installed into. This applies to both the account being used to install the agent and to the Action account specified.

The recommended approach for installing agents is using the Install/Uninstall Agents Wizard in the MOM Administrator console. This wizard provides the options to configure an installation account and/or an Action account. The installation account specified must have the administrative credentials to install the agent on the target computer(s), and the Action account must have the permissions required to perform the actions the agent requires such as collect data from providers and run automatic responses such as scripts. The default account used by the agent during installation is the Management Server Action account specified during the management server installation. This account can be used if it has administrative credentials on the target systems. For additional recommendations regarding the Action account see Chapter 11, "Securing MOM."

For example, let's take the Contoso and Coyote domains, which do not have trusts between them and are in separate forests as shown in Figure 5.8. If the management server (Monarch) exists in the Contoso domain and the servers to be monitored exist in the Coyote domain, the account that installs the agent will need to have permissions in the Coyote domain.

In this example the installation account belongs to the Domain Administrators group within the Contoso domain. The Action account specified is a member of the local Administrators group on the Fountain and Monarch servers. These accounts are specified during agent installation from the MOM Administrator console.

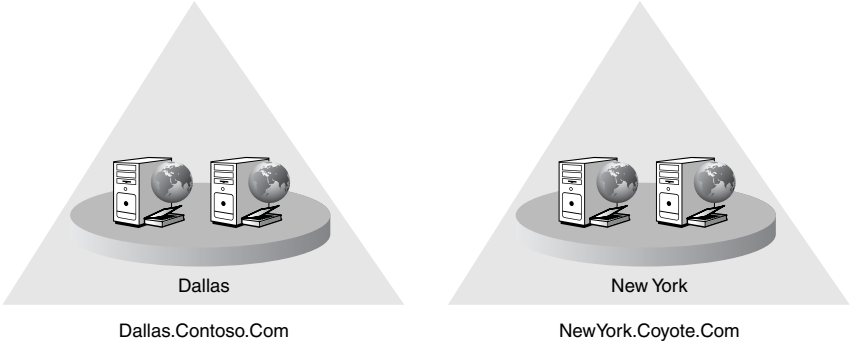


FIGURE 5.8 Multiple domains.

As part of your planning, you should identify or create accounts that will have the necessary permissions to install the MOM agents and perform MOM actions on the servers being monitored. In Chapter 9, "Installing and Configuring Agents," we discuss agents and the details of installing and configuring agents.

The decision of whether to enable mutual authentication is a key design choice that needs to be made during the planning stage. Mutual authentication provides authentication and encryption for the information sent from the MOM agent. The decision of whether to enable mutual authentication depends highly on your domain and trust configuration and whether you will be monitoring systems in a workgroup configuration. Details on mutual authentication (including when to enable it) are provided in Chapter 11.

Connecting MOM

Out-of-the-box MOM 2005 provides strong management capabilities for Microsoft-based products. Because few organizations are homogeneous, Microsoft provides two primary methods to connect MOM to other products: Product Connectors and the MOM Software Development Kit (SDK):

- Product Connectors exist to connect MOM to third-party management solutions.
- The MOM SDK is a .NET library for developers to use when programming integration with MOM 2005.

As the size of the organization grows, the need for integration into other management platforms grows as well. If your organization is large, there is likely to be a trouble ticketing application and another management console already existing in the environment. The design needs to take into account how to integrate with these other management applications.

There are really two main methods, depending on the requirements. These are alert forwarding or alert synchronization. The design should clearly specify the requirements and the chosen methods for handling integration with the other management platforms.

Alert Forwarding

Alert forwarding works well in environments where MOM only needs to have MOM-generated alerts sent to the other management system. These alerts could also be forwarded from the other management system to MOM. The key element to alert forwarding is that after the alert is forwarded, there is no follow-up.

Although this may seem draconian at first glance, it is common. It is the basis for the original management protocol, Simple Network Management Protocol (SNMP). SNMP traps are generated on alert conditions and simply forwarded off to the SNMP management server.

There are various methods that MOM can use to forward alerts to another management system, depending on what the management system accepts. The methods include the following, in order of increasing sophistication:

- Send an SNMP trap.
- Execute a command or batch file.

- Launch a script.
- Call a method on a managed code assembly.

These methods can pass the information on the third-party management system as a response to an alert using an alert rule. They are simple to implement and easily adapted to most management systems.

Product Connectors and Alert Synchronization

In some cases, the alerts need to be connected in both systems. You want to be able to update the status of the alert in the third-party management system and have that reflected in the MOM alert. This is the case where you need true integration of management systems, MOM and the third-party management system. An example of this is a trouble ticket system, where you would want to have alerts generated in MOM create tickets in the trouble ticket system. However, as the status of the MOM alert changes, you want the trouble ticket status to update as well. Also, if the ticket is closed out in the trouble ticket system, you want the alert to be resolved in MOM.

This requires synchronizing alerts, which is accomplished using the MCF. The connectors run on the management servers and require significant planning, potentially the cost to purchase or develop the connectors, and configuration. However, they provide a tremendous value when implemented correctly.

Many organizations use third-party systems management software to monitor their computing resources. Product connectors are designed to transfer information between these management software packages and MOM 2005. Microsoft provides a number of product connectors that are available for download from Microsoft's website at http://go.microsoft.com/?linkid=4335769. Some of the product connectors that currently exist include

- **Tivoli**—Allows alerts to be forwarded to Tivoli TEC and synchronized between MOM and Tivoli
- **HP OpenView**—Provides unidirectional and bidirectional communication between MOM and HP OpenView
- **HP Network Node Manager**—Configures MOM to send alerts to HP Network Node Manager

These connectors are the primary method for providing coexistence between MOM and other monitoring solutions. There are two major benefits to these types of connectors:

- MOM rules and knowledge (available via many management packs) can be provided to other products.
- Product connectors extend MOM 2005's capabilities.

Help Desk Solutions

Product connectors are not used only for connecting management software packages to MOM 2005. Several third-party connectors on the Microsoft Operations Manager Product Connector site (http://go.microsoft.com/?linkid=4335769) integrate help desk solutions with MOM 2005.

Some of the help desk solutions available with connectors include Amdocs Clarify, CA Solve, Peregrine Service Center, Remedy ARS, Tivoli Service Desk, and Vantive. These products provide creation of tickets based on alerts received by MOM 2005.

Based upon the deployment stages discussed in Chapter 4 (assessment, design, planning, POC, pilot, implementation, and maintenance), there are multiple phases where product connectors may to be built into your MOM planning.

Product connectors should be discussed during the assessment phase, and you should determine whether there is a business requirement for their deployment. If a particular product connector is necessary, the specifics of the connection should also be assessed—including which connector is required, what server MOM will communicate with, and whether alerts will be forwarded in one or both directions. This information is then integrated into the design document to describe how the product connector will be implemented.

The planning stage is where the majority of the work takes place related to deploying the product connector. Here the tasks that will occur during the POC, pilot, and implementation steps are determined. To effectively deploy a product connector we recommend that you also deploy it as part of your POC environment. In the case of a product connector, this requires that a server in the POC environment run the third-party management solution. Testing the product connector during a POC is suggested rather than first trying to incorporate it in your production environment.

Download, install, configure, and document the process for the product connector as part of the POC. After the product connector is functional, test the connector to verify that alerts are being forwarded between MOM and the third-party management tool. Finally, within the pilot stage use the document you created that describes the download, installation, and configuration for connecting to the production third-party management solution.

MOM SDK

There are times when MOM cannot match the business requirements you have identified without having to extend its functionality. To address this Microsoft has provided the MOM 2005 SDK. At a high level, the SDK can be used to synchronize MOM alerts, extend MOM rules, and provide external interfaces to MOM.

The focus of this chapter is not to provide thorough information on the SDK (which will be discussed in more detail in Chapter 19), but to determine where you should plan to use the SDK as part of your deployment. If the SDK needs to be used as part of the MOM

2005 environment, this should be identified during the assessment stage. For example, if the environment requires a custom solution (a custom management console, custom reports, or custom management packs) the SDK should be identified as a potential tool. During the assessment phase SDK requirements should be identified and specified as much as possible to provide effective information for the design. During the design stage these custom requirements should be included as part of the design document.

Actual creation of the customized solution should occur during the POC stage. Within the POC, the solution can be created and tested without potential impact to the production environment. The solution should be evaluated during the POC phase and updated to validate that it effectively meets your business requirements. The custom solution should be deployed into the production environment as part of the pilot stage and rolled into full production during the implementation phase.

Summary

This chapter provided information on the challenges associated with deploying MOM 2005 in complex configurations that include redundancy, multitiered or multihomed implementations, or product connectors. The next chapter discusses how to install MOM 2005 in your proof of concept, pilot, or production environments.

This page intentionally left blank

CHAPTER 6

Installing MOM 2005

IN THIS CHAPTER

- Planning Your Installation
- Installation Prerequisites
- Performing the Installation
- Installing Additional Components
- Troubleshooting Tips

This chapter discusses the procedures to install a new Microsoft Operations Manager (MOM) 2005 environment on a Windows 2000 Server or Windows Server 2003 operating system. We explain MOM 2005 installation prerequisites, the different server roles, and hardware requirements for each role. We also discuss database options, the function of the domain controller, and various security considerations. We will go through two scenarios for a MOM configuration and installation and discuss potential troubleshooting areas. This chapter provides the information to successfully install a "simple" configuration of MOM 2005.

Focus of This Chaper

This chapter discusses the requirements and procedures to install MOM 2005 into a management group with a single management server. More complex implementations including multiple management servers and clustered database configurations are discussed in Chapter 10, "Complex and High Performance Configurations."

Planning Your Installation

Before actually running the MOM setup program, you need to determine what your operations management environment will look like. As part of the planning discussion in Chapter 4, "Planning Your MOM Deployment," and Chapter 5, "Planning Complex Configurations," you should have considered the following questions:

- Which computer will run the MOM core components?
- Which computer will host the MOM database?

- Will you be installing MOM Reporting? Which system will host the MOM reporting server?
- What is the operating system environment? A management server installed on Windows 2000 has somewhat different security options than one using Windows Server 2003.
- How many servers will you want to manage? What type of activities do these servers perform?

Prior to your installation, be sure to read through the planning chapters of this book for a discussion of planning-related topics.

Installation Prerequisites

A MOM 2005 environment includes the core components of the MOM database, at least one MOM management server, and MOM Administrator and Operator consoles. Optional components include the MOM Web console and MOM Reporting.

As discussed in Chapter 4, in a large production environment you may decide to split out different MOM components to separate servers. The more computers MOM has to manage, the higher the resource requirements, so separating the server roles gives you some flexibility in machine configurations. Optimal configuration of your MOM installation will depend on your particular operational environment.

To assist with the installation process, Microsoft includes a prerequisite checker utility with the MOM installation program. This utility lets you know of any deficiencies in your proposed MOM environment prior to installation. The prerequisite checker creates a report you can use to verify that the intended computer meets the hardware and software requirements for MOM 2005.

MOM Server Roles

This section reviews the functions of the different servers in a MOM environment. For purposes of this chapter we will assume a single MOM management server; more complex configurations are discussed in Chapter 10.

Management Server

The MOM software is installed on the management server, which is the central computer in your MOM environment. A management server includes the roles of the DAS, the MOM server, and the MOM agent components. These functions were previously discussed in Chapter 3, “How Does It Work?” You should use a dedicated computer to host the management server. The management server has the hardware and software requirements listed in Table 6.1. These requirements apply to MOM 2005 with Service Pack 1 (SP1).

TABLE 6.1 System Requirements for Each MOM Management Server

Hardware		
	Minimum	**Recommended**
Processor	Intel Pentium-compatible 550 megahertz (MHz) or higher processor	Dual Intel Pentium-compatible 450MHz or higher processor
Memory	512MB of RAM	1GB of RAM
Disk space	5GB of hard disk space	
Software		
	Minimum	**Recommended**
Operating system	One of the following: Windows Server 2000 family with the latest service pack Windows Server 2003 family with the latest service pack	Windows Server 2003, Enterprise Edition with the latest service pack
Additional software	MDAC version 2.8.1022.0 or later Microsoft .NET Framework 1.1	

Database Server

The database server stores configuration and operational data used by the MOM environment. For production environments, the recommended engine is Microsoft SQL Server 2000 or above. Using the database server with the SQL Server 2005 engine is supported with MOM 2005 SP1 and requires three hotfixes (see http://support.microsoft.com/kb/917615/ for additional information). See the "MOM 2005 with SQL Server 2005 Implementation Steps" sidebar later in this chapter for additional information on installing MOM 2005 with SQL Server 2005.

For small test configurations, you may choose to use SQL Server 2000 Desktop Engine (MSDE) or SQL Server 2005 Express Edition instead of SQL Server.

SQL Server Placement

As discussed in Chapter 4, for larger production systems a best practice is to install the MOM database on a dedicated computer.

Table 6.2 gives the system requirements for the computer hosting the MOM database.

TABLE 6.2 System Requirements for the Database Server

Hardware		
	Minimum	**Recommended**
Processor	Intel Pentium-compatible 550MHz or higher processor	Dual Intel Pentium-compatible 450MHz or higher processor
Memory	512MB of RAM	1GB of RAM (more is always better)

TABLE 6.2 Continued

Hardware		
Disk space	5GB of hard disk space	15GB of hard disk space (30GB maximum supported)
Software		
	Minimum	**Recommended**
Operating system	One of the following: Windows Server 2000 family with the latest service pack Windows Server 2003 family with the latest service pack	Windows Server 2003, Enterprise Edition with the latest service pack
Additional software	Microsoft SQL Server 2000, Standard or Enterprise Edition, with SP3a or later with all post Service Pack hotfixes	One of the following: Microsoft SQL Server 2000, Standard or Enterprise Edition with SP4 Microsoft SQL Server 2005, Standard or Enterprise Edition with the latest service pack

Before installing the MOM database, you must install and configure SQL Server on the computer that will host the database server. Particulars of the SQL Server installation should include

- Selecting database authentication to be Windows only
- Configuring TCP/IP as the network protocol
- Configuring the SQL Server (MSSQLSERVER) and SQL Server Agent (SQLSERVERAGENT) services to run and start automatically when the computer starts.

Different Service Names with SQL Server Instances

The service names for the Microsoft SQL Server services are different if you have named instances of SQL Server: the format would be MSSQL$< *instance name*> and SQLAgent$< *instance name*>.

Consoles

The MOM Administrator and Operator consoles are automatically selected for installation when you install the management server. You may also install these consoles on other computers. This section describes the MOM consoles and their system requirements.

Administrator Console

The MOM Administrator console is used for configuring the MOM environment and maintaining the management packs.

Operator Console

The Operator console is used to view and resolve alerts that have been identified to MOM. It also includes topographical views of your environment and the capability to run tasks against different servers and components.

Table 6.3 lists system requirements for the Administrator and Operator consoles.

TABLE 6.3 Administrator and Operator Console Requirements

Hardware		
	Minimum	**Recommended**
Processor	Intel Pentium-compatible 550MHz or higher processor	Intel Pentium-compatible 1GHz or higher processor
Memory	128MB of RAM	256MB or more of RAM
Disk space	150MB of hard disk space	
Display	Windows 2000–compatible video graphics adapter with a resolution of 800x600 and capable of displaying 256 colors	Windows 2000–compatible video graphics adapter with a resolution of 1024x768 and capable of displaying 24-bit color or greater
Software		
	Minimum	**Recommended**
Operating system	One of the following: Windows Server 2000 family with the latest service pack	Windows Server 2003 family with the latest service pack
	Windows XP Professional with the latest service pack	Windows XP Professional with the latest service pack
	Windows XP 64-Bit Edition with the latest service pack	
Additional software	Microsoft .NET Framework 1.1	

MOM Web Console

The optional Web console requires Internet Explorer 5.5 or later on the remote system where you will use the MOM Web console. Additionally, the following software is to be installed on the management server:

- Internet Information Systems 5.0 (Windows 2000 Server family) or 6.0 (Windows Server 2003 family)
- ASP.NET
- Network COM+ access

SQL Server 2000 Reporting Services Server Requirements

MOM 2005 Reporting uses SQL Server Reporting Services (SSRS). You must install and configure SSRS prior to installing MOM 2005 Reporting. These two components can be

on the same server. Table 6.4 lists the requirements for SSRS. MOM Reporting requires the full edition of MOM 2005 and cannot be installed with MOM 2005 Workgroup Edition.

TABLE 6.4 SQL Server Reporting Services Requirements

Hardware		
	Minimum	**Recommended**
Processor	Intel Pentium-compatible 550MHz or higher processor	Intel Pentium-compatible 1GHz or higher processor
Memory	256MB RAM	1GB or more of RAM (more is always better)
Disk space	10GB of hard disk space	
Software		
	Minimum	**Recommended**
Operating system	One of the following: Windows Server 2000 family with the latest service pack Windows Server 2003 family with the latest service pack	Windows Server 2003, Enterprise Edition, with the latest service pack
Database software	Microsoft SQL Server 2000, Standard or Enterprise Edition with SP3a or later Microsoft SQL Server 2000 Reporting Services with SP1	Microsoft SQL Server 2000, Standard or Enterprise Edition with SP4 Microsoft SQL Server 2000 Reporting Services with SP2 Or Microsoft SQL Server 2005 Standard or Enterprise Edition with the latest service pack Microsoft SQL Server 2005 Reporting Services
Additional software	Internet Information Systems 5.0 (Windows 2000 Server family) ASP.NET 1.1 (requires Microsoft Framework 1.1 installation on Windows 2000 servers) Visual Studio .NET 2003 to use Report Designer capabilities	Internet Information Systems 6.0 (Windows Server 2003 family) ASP NET 2.0 with SSRS 2005
Software		

TABLE 6.4 Continued

	Minimum	Recommended
To view MOM reports	One of the following: Microsoft Internet Explorer 5.5 with SP1 or SP2 Microsoft Internet Explorer 5.01 with SP2 Netscape 7.0 Netscape 4.78	Microsoft Internet Explorer 6.0 with SP1
To create or customize reports	Microsoft Visual Studio .NET 2003, or Integrated Developer Environment 2003	

SSRS Incompatibility with Windows 2000 Domain Controllers

Do not use a Windows 2000 domain controller to host the report server. The setup process does not finish successfully when the computer is a domain controller.

MOM Reporting

Table 6.5 lists the requirements for the MOM Reporting server.

TABLE 6.5 MOM Reporting Server Requirements

Hardware		
	Minimum	**Recommended**
Processor	Intel Pentium-compatible 550MHz or higher processor	Intel Pentium-compatible 1GHz or higher processor
Memory	512MB RAM	1GB or more of RAM
Disk space	200GB of hard disk space (based on grooming from operational database)	
Software		
	Minimum	**Recommended**
Operating system	One of the following: Windows Server 2000 family with the latest service pack Windows Server 2003 family with the latest service pack	Windows Server 2003, Enterprise Edition, with the latest service pack
Database software	Microsoft SQL Server 2000, Standard or Enterprise Edition with SP3a or later	Microsoft SQL Server 2000, Standard or Enterprise Edition with SP4 Or Microsoft SQL Server 2005, Standard or Enterprise Edition with the latest service pack

Service Pack Compatibility Between MOM 2005 and Windows Server 2003
MOM 2005 is certified against the base version of Windows Server 2003 and was released prior to Windows 2003 service pack maintenance. If you have implemented Windows Server 2003 SP1 we recommend you use MOM 2005 SP1. A number of issues exist when running the Released-to-Manufacturing (RTM) version of MOM 2005 on a Windows 2003 SP1 platform.

If you use Windows 2003 Service Pack 1 but do not plan to immediately apply MOM 2005 SP1 to your MOM installation, search the Microsoft knowledge base at http://support.microsoft.com for article 898921, which provides a consolidated summary of the known issues and hotfixes when running the base version of MOM 2005 with Windows 2003 SP1.

Service Packs Approach

In general, although service packs address bug fixes, they also tend to introduce new sets of features and issues. This will be true for operating systems and monitored applications as well as MOM itself. Always thoroughly test service packs before introducing them to a production environment.

Unsupported Configurations

There are a number of configurations that Microsoft officially does not support with MOM 2005 SP1:

- Any changes to the MOM database or MOM reporting database schema.
- DEC Alpha hardware.
- Internet Protocol Version 6 (IPv6).
- Bidirectional, complex script languages, such as Arabic or Hebrew.
- A Multilingual User Interface (MUI) release for MOM.
- Running MOM 2005 without the MOM 2005 SP1 Management Pack.
- Multiple MOM databases connected to a single MOM reporting database or for multiple MOM reporting databases connected to a single MOM database.
- More than one MOM reporting database per management group.
- Running Computer Discovery to install an agent on the same computer where you are running Computer Discovery.
- Installing MOM 2000 SP1 agents after the MOM environment is upgraded to MOM 2005 SP1. MOM 2000 SP1 agents are supported only during the upgrade process.
- Agents on Windows NT 4.0 are not supported. These agents must be uninstalled and Windows NT 4.0 systems monitored agentlessly. (More information is available in Chapter 9, “Installing and Configuring Agents,” and the Microsoft Operations Manager 2005 Deployment Guide.)
- Moving a MOM deployment from one domain to another. Moving to another domain—or renaming the domain—requires uninstalling all the MOM components and then reinstalling MOM in the new domain.

Database Options

Although the MOM database (OnePoint) can utilize either a Microsoft SQL Server database or the no-cost versions of SQL Server 2000 MSDE or SQL Server 2005 Express Edition, for all but the smallest environments we recommend you use the full version of SQL Server. The no-cost versions have limits on the database size (MSDE has a maximum database size limit of 2GB, and Express's maximum size is 4GB) and cannot be used for MOM Reporting.

Calculating database size was discussed in Chapter 4. The size involves a number of factors, including the following:

- How many computers you plan to manage
- How much data you plan to collect, including events, alerts, and performance data
- The management packs you will deploy
- How often you will groom your MOM database

The maximum supported size for the OnePoint database is 30GB.

Real World—Optimal Database Size

For optimum performance, it is recommended to keep your database size below 15GB because a smaller database responds more quickly to events and alerts. Many installations report that keeping the database below 16GB is essential, and that constraints with Data Transformation Services (DTS) package transfers and other performance issues advocate never having a production MOM database larger than 20GB.

This is not to say that you may not encounter a large production database, but maintaining an effective monitoring environment with a large database requires constant and detailed tuning.

The setup process by default sets the size of the database file to 1GB and the log file to 20% of the size of the database file (200MB). The MOM database is a fixed size: *Do not enable automatic file growth; it can keep the MOM database from functioning properly*. You can expand the database manually; this technique is described in article 300119 at the Microsoft Support website, http://support.microsoft.com/kb/300119/.

More Information About KB 300119

Although this article is written for MOM 2000 SP1, it applies to MOM 2005 in a SQL Server 2000 environment. The process is similar for SQL Server 2005. Although the article does not say you need to stop the MOM service, we suggest you do so while extending the database.

Estimating Sizing

You can refer to the MOM Sizer and the *Microsoft Operations Manager 2005 Performance and Sizing* white paper, previously referenced in Chapter 4, to assist in estimating database size.

TechNet subscribers also can use the System Capacity Planner 2006 tool at no cost. The Capacity Planner helps size and plan deployments for MOM 2005 (and Exchange 2003). More information on the planner can be found at http://www.microsoft.com/windowsserversystem/systemcenter/sccp/.

Database Placement

The database server can be on the same machine as the management server or on a separate machine, although in Chapter 4 we recommend deploying it on a separate server for performance or fault-tolerance purposes. Additional fault-tolerance can be achieved by using database clustering or other SQL Server fault-tolerance methods. Clustering the MOM databases is discussed in Chapter 5, "Planning Complex Configurations," and Chapter 10, "Complex and High Performance Configurations."

Order of Installation

Should the database server be installed on a separate system from the management server, this must be done prior to installing the management server, or the MOM installation task will fail.

The Domain Controller

MOM must be installed in a Windows Server domain environment, but the servers that it manages do not necessarily need to be in the domain.

With MOM 2000, you were not able to install the MOM server software on a domain controller. This restriction was put in place for security reasons. That restriction has been relaxed with MOM 2005, and you can install any MOM component on a domain controller, although there are some caveats. The following considerations should be taken into account when installing to a domain controller:

- The MOM database and the MOM reporting database must be on the same computer.
- If the management server is on a domain controller, you cannot have another management server in that same management group.
- Product connectors (covered in Chapter 19, "Interoperability") may not function correctly.

Security Considerations

You must create and configure two service accounts prior to installing the MOM core components. This section describes the Data Access Server (DAS) account and the Management Server Action account used by the management server.

Configuring the DAS and Management Server Action Accounts

It is not recommended to use the same domain user account for both service accounts. With the same user account, the DAS account not only has privileges on the MOM database but also on the management server and managed computers. Using separate accounts allows you to restrict the DAS account's privileges to the MOM database.

The MOM setup process grants the required rights to these two accounts.

DAS Account

The DAS account is used in conjunction with the Data Access Server role and provides centralized access to the MOM database. During installation, MOM assigns this account to the correct security group and SQL Server role required for the DAS.

About the DAS Account

The DAS account requires access to the OnePoint database. As part of the MOM 2005 installation process, the DAS account is given the "db-owner" (database owner) role for the OnePoint database and SQL Server Security Login with "Permit" server access. For MOM Reporting, the DAS account must also be a member of the SC DW DTS security groups on both the MOM database server and the MOM reporting server. Members of this security group can perform data archiving functions from the MOM 2005 operational database to the MOM 2005 reporting database.

Security Requirements

The credentials under which to run the DAS account vary based on the operating system you are using and where the MOM database and management server components are located. Table 6.6 shows the recommended options.

TABLE 6.6 Security Credentials for the DAS Account

MOM Components	Windows 2003	Windows 2000
MOM database and management server on same system	Local Service	Local User Account
MOM database and management server on separate systems	Network Service	Domain User Account

Security Alert

The Local System account should not be used for the DAS account. It has full access to the system, including the Directory Service on domain controllers.

For more information regarding the Local Service, Local System, and Network Service accounts, see http://go.microsoft.com/fwlink/?LinkId=50019.

Management Server Action Account

The Management Server Action account performs a number of roles:

- Running computer discovery and automatically installing agents
- Communicating with, collecting data from, and running actions on, agentless managed computers
- Collecting data from the registry, performance counters, and event logs of the local computer the management server is installed on

Group Membership for the Management Server Action Account

The Management Server Action account can be a member of the Domain Admins group, but for maximum security it should be a Domain User and a member of the local Administrators group on each computer it deploys agents to.

Additional information on both of these accounts is available in Chapter 11, "Securing MOM."

Performing the Installation

Now it's finally time to actually install MOM! We'll step through installing MOM in two configurations: the single server configuration and a configuration where the database server is on a separate machine. Remember that more complex configurations with multiple management servers are covered in Chapter 10.

MOM 2005 and SQL 2005

The release of MOM 2005 was prior to that of SQL Server 2005, and Microsoft documentation focuses on SQL Server 2000 with the MOM operational and reporting databases. In 2006, Microsoft announced support of the newer version of SQL Server with Operations Manager. You can now install MOM 2005 with either version of SQL Server. Existing installations can choose to stay with SQL Server 2000, migrate to the new version, or upgrade the database components to SQL Server 2005.

Installation Overview

The actual process involved in installing MOM 2005 is the same regardless of the complexity of the configuration. The steps required are as follows:

1. Install Microsoft SQL Server 2000 with Service Pack 3a or above on the server intended to be the MOM database server. We will concentrate here on SQL Server 2000 because that is the version documented by Microsoft. The installation process for MOM with SQL Server 2005 is discussed in the "MOM 2005 with SQL Server 2005 Implementation Steps" sidebar later in this chapter.
2. Run the Check Prerequisites utility to verify that the server meets hardware and software prerequisites.
3. Run the MOM installation wizard to install MOM 2005 components.
4. In a more complex configuration, for each component you install on a separate server you should repeat steps 2 and 3 for that server as well.

As we go through the installations for the different scenarios, the preceding steps are referred to in each configuration.

SQL Server 2000 Service Pack Maintenance

MOM 2005 requires that SQL Server 2000 Service Pack 3a (SP3a) or above must be applied to your SQL Server installation. Service Packs for Microsoft SQL Server can be downloaded from http://www.microsoft.com/sql/downloads/servicepacks.asp.

Microsoft distributes bug fixes in service packs. Service packs are cumulative; each new service pack contains all the fixes from earlier service packs for that version of software, plus any new fixes. You do not need to install a previous service pack before you install the latest one. For example, SQL Server 2000 SP4 includes all fixes from previously released service packs 1 (SP1), 2 (SP2), and 3a (SP3a). The most recent version of a service pack can be applied to an original installation or to an installation where earlier versions of the service pack were previously applied.

Identifying SQL Server versions

The process of identifying the installed SQL Server Service Pack Version and Edition of SQL Server is described in KB article 321185, available at the Microsoft support website at http://support.microsoft.com/kb/321185/.

Single Server Configuration

This example considers a single server configuration with all MOM 2005 components running on a server named Monarch. Monarch will be the management server and host the MOM database, and will have the only Administrator console in the environment. Figure 6.1 illustrates a single management server (Monarch) environment.

FIGURE 6.1 Single server configuration of MOM 2005.

For the single server configuration, we will perform the basic three installation steps on Monarch. Because Monarch will contain the database server, we need to have SQL Server 2000 with Service Pack 3a or above installed on the server prior to running the MOM setup program. We will then run the Check Prerequisites utility and run the MOM installation setup task. The steps are as follows:

1. To install MOM, first log on to the computer you have identified as your management server using administrative credentials. *This will be the Monarch server.*
2. Make sure that SQL Server 2000 with SP3a or above is installed; SP4 is recommended.
3. Run the MOM Setup program.

You can run Setup from either the MOM 2005 CD or a shared network installation point. If you are using a CD-ROM, inserting the disk causes Setup to start automatically. If you are installing over the network, you will have to find and run setup.exe, which should be in the root of the MOM installation directory. The first screen of the setup program, (see Figure 6.2) shows you the options available as setup tasks:

1. Run the Check Prerequisites utility, the first item on the Setup Tasks tab of the Microsoft Operations Manager 2005 Setup Resources screen. Based on the components you select, the prerequisite checker will verify that the hardware and installed software meet the installation requirements for MOM 2005.
2. Because we are planning a Typical installation of the MOM components and database onto a single server, select the first option on the Check Prerequisites screen, which is the Microsoft Operations Manager 2005 Components option and its subcomponents; then click Check to run the prerequisite checker, as shown in Figure 6.3. The MOM Connector Framework and MOM 2005 Web Console are not required components, and because we are not installing them at this time these items are not selected.

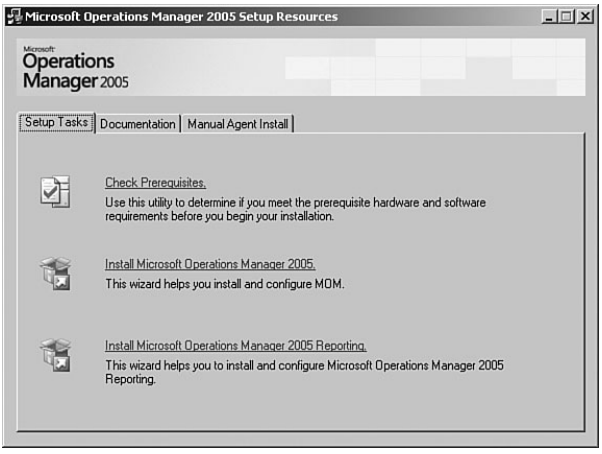


FIGURE 6.2 The opening splash screen.

Moving the MOM Database

If necessary you can later move the OnePoint database to a new location. The process to move the OnePoint database without reinstalling the management server(s) is described in article 917894 at the Microsoft Support website, located at http://support.microsoft.com/kb/917894/.

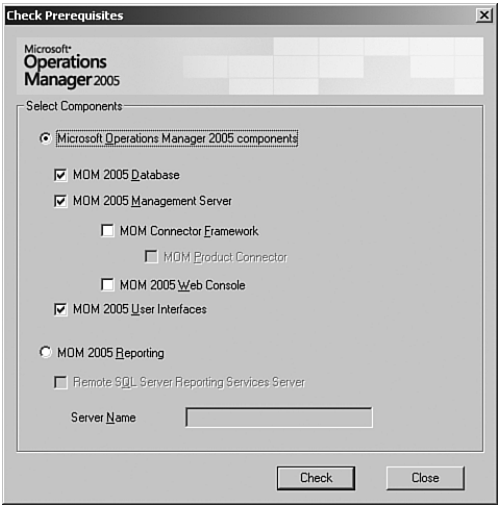


FIGURE 6.3 Check Prerequisites utility for MOM components.

3. The resulting report, illustrated in Figure 6.4, shows you which components were tested and whether or not they passed the installation prerequisites. The status indicators are of a red light/yellow light/green light variety. If you have any failures (stop signs), you cannot proceed. Warning signs indicate issues that setup will not block but should be looked into, and a green light indicates it is safe to proceed. If you have any failures (and/or warnings you want to address), go ahead and correct those issues. Then rerun the prerequisite checker until all systems are "go."

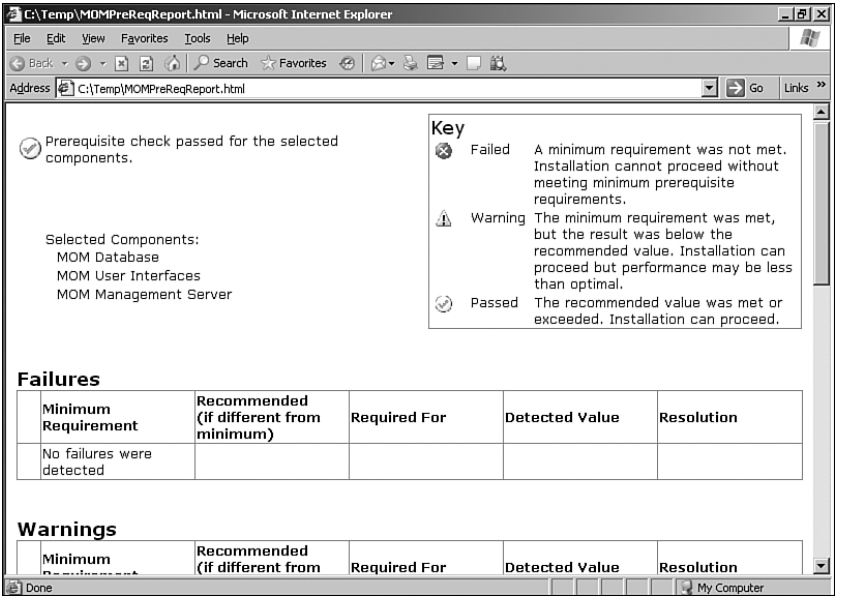


FIGURE 6.4 Results from the prerequisite checker.

You are now ready to proceed to the next installation task, installing MOM itself. This is the second item on the Setup Tasks tab of the Microsoft Operations Manager 2005 Setup Resources splash screen. To avoid any potential resource conflicts, be sure to close any other open programs running on your system; then select the Install Microsoft Operations Manager 2005 task and follow these steps:

1. The first few screens of the installation wizard are fairly typical. You will accept the license agreement and enter user information and your product key. The first screen where you have to consider your preferences is the Installation Options screen. Here you can select Typical (for a single server install) or Custom (when installing components on multiple servers). To install a single server only, select the Typical option, shown in Figure 6.5.

2. The prerequisite checker automatically performs a last-minute verification; if there are no outstanding issues in terms of hardware or software prerequisites the installation proceeds, with the next step being the database setup. The installation will not

continue if there are any failed prerequisites. If errors were detected, implement the resolutions suggested in the report output from the prerequisite checker and rerun the installation step.

FIGURE 6.5 Installation options.

Bypassing the Prerequisite Checker

Occasionally there may be a need to bypass the automatic prerequisites check as part of the MOM installation. In this case run the prerequisite check by itself (the first item on the Setup Tasks list) to verify that you have met the requirements. Then run the install silently using the MSIEXEC command to install the database components, including the switch `/PREREQ_COMPLETED=1` to bypass the automatic check. One example where this would be necessary is if you are using SQL Server 2000 SP4 and MOM 2005 without SP1. More information is available at http://support.microsoft.com/kb/902803/.

3. You will be asked about database specifics—to select the database instance onto which you want to put the OnePoint database, and to confirm the size and location of the data and log files.

4. Next, you specify the management group name. This name cannot be modified after MOM is installed. To modify the name after installation, you will have to remove all MOM components and reinstall them!

   The management group name is alphanumeric. You can choose a name based on geographical locations, organizational departments, or administrative requirements. The management group name must be unique; if you configure additional management groups, each one must have a unique name. Figure 6.6 shows the Management Group Name screen.

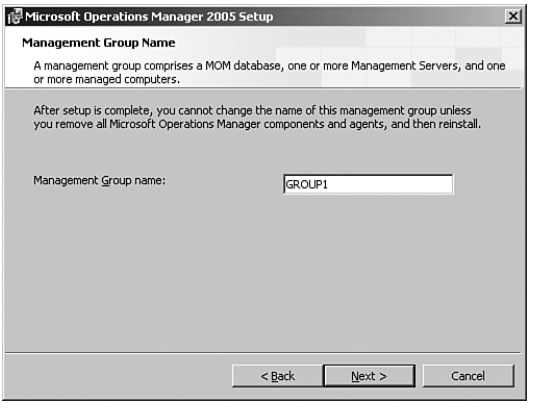


FIGURE 6.6 The Management Group Name screen.

5. Specify the Management Server Action account, as illustrated in Figure 6.7. As described in the "Management Server Action Account" section earlier in this chapter, the Management Server Action account is used for several functions. It runs computer discovery, collects data, and communicates with agents on managed computers.

Security Alert

If you specify an account that is a member of the Domain Admins group, you are warned that this is a security risk.

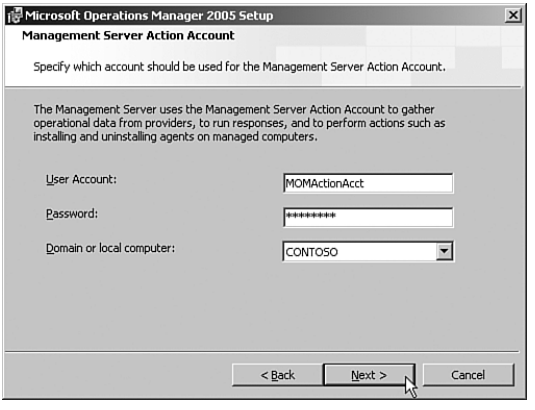


FIGURE 6.7 Specifying the Management Server Action account.

6. As shown in Figure 6.8, specify the service account you have previously created that will be used to access the OnePoint database.

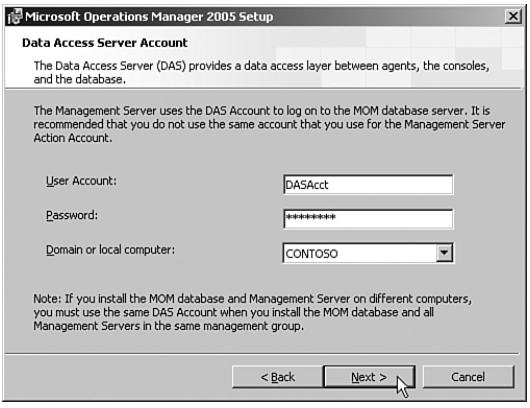


FIGURE 6.8 Specifying the Data Access Server account.

7. On the MOM Error Reporting screen, check the Enable Error Reporting option and take the default of Automatically Send Reports to Microsoft.

Enabling Error Reporting

Automatically sending reports to Microsoft enables Microsoft to be alerted of potential bugs in its software and provides troubleshooting data related to the specific error condition.

8. Select the appropriate Active Directory option for your environment and this particular management group, as illustrated in Figure 6.9:

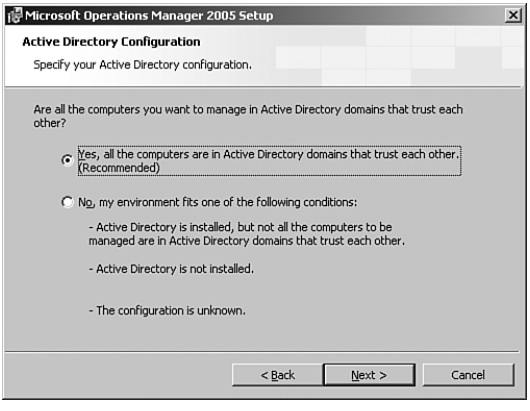


FIGURE 6.9 Specifying your Active Directory configuration.

- If the domains are in the same Active Directory Forest, trusts exist automatically. If the domains belong to different forests that trust each other, choosing Yes allows

MOM to use mutual authentication for all communication between management servers and agents. Mutual authentication means that the management server and the agent will authenticate each other before any communication occurs.

- Selecting No means that mutual authentication will not be used.

At this point you have specified all necessary options, and the installation process will proceed.

Separate Database Configuration

With the separate database server configuration, we will install MOM 2005 with all MOM 2005 components running on a server named Monarch, with the exception of the MOM database server which is running on Fountain. Monarch is the management server and includes the Administrator and Operation consoles. Fountain is a single server (nonclustered) that processes the MOM 2005 database services. Figure 6.10 illustrates a two-server MOM configuration using a separate database server.

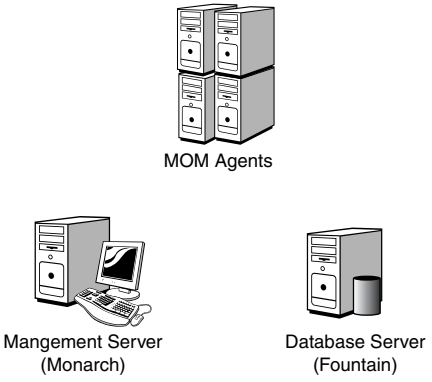


FIGURE 6.10 MOM 2005 with a separate database server.

Separate MOM Database Server

Here you will go through the basic installation steps (checking that Microsoft SQL Server is on the server intended for the MOM database server as previously described in the "Single Server Configuration" section, running the Check Prerequisites utility, and running the MOM installation wizard) on the database server, but you will install only the MOM database component. You will then repeat the steps of running the Check Prerequisites utility and running the MOM installation task program for the management server, as already outlined in the previous single server configuration. The steps are as follows:

1. To install MOM, first log on to the computer you have identified as your database server using administrative credentials (in this example "Fountain").

2. Make sure that SQL Server is installed.
3. Start the MOM setup program. You can run setup from either the Microsoft Operations Manager 2005 CD or a shared network installation point.
4. Run the Check Prerequisites utility, previously described in this chapter. Based on the components you select, the prerequisite checker will verify that the hardware and installed software meet the installation requirements.

   Because we are planning to install the MOM database onto a separate server, on the Check Prerequisites window select the Microsoft Operations Manager 2005 components option with only the MOM 2005 database component selected; then click Check to run the prerequisite checker, as illustrated in Figure 6.11.

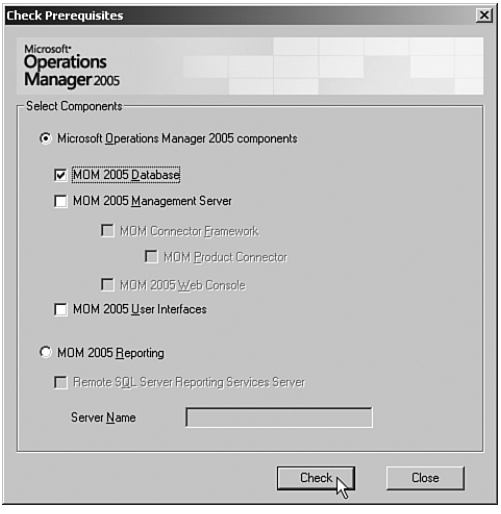


FIGURE 6.11 Check prerequisites for the MOM database component.

The resulting report shows the components on which you ran the prerequisite check (in this case, the MOM database), and whether the installation prerequisites were met. The statuses will be a red light/yellow light/green light. If you have any failures, go ahead and correct those and rerun the prerequisite checker until all systems are "go."

Installing the OnePoint Database on Another Server You are now ready to proceed to the next installation task, which is to install the OnePoint database to a separate server, named Fountain. Close the Check Prerequisites window and select the second task on the splash screen to initiate the Microsoft Operations Manager 2005 installation wizard. Be sure you have no other programs running on your system. Follow these steps:

1. The first few screens of the Microsoft Operations Manager 2005 install wizard are fairly typical. Accept the license agreement and enter user information and your product key.
2. On the Installation Options screen, select the Custom option because we are installing the database component on another server. This option takes you to the Custom Setup screen where you can select various MOM components for installation.
3. Make sure that only the MOM 2005 Database is selected as shown in Figure 6.12 and click Next to continue to the next step.

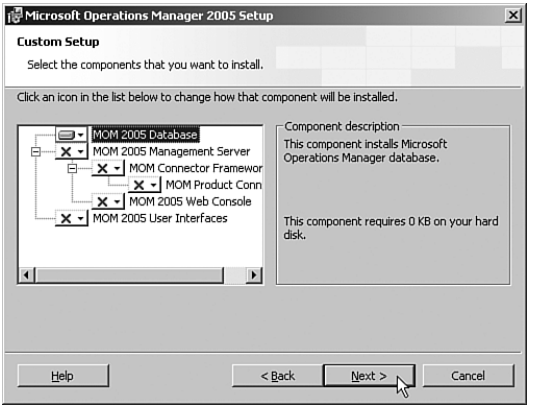


FIGURE 6.12 Custom setup for the MOM 2005 database.

4. The MOM setup program automatically runs the prerequisite checker as a last-minute verification; if there are no issues, you can proceed with the installation process.
5. Select the database instance to which you want to put the OnePoint database and confirm the size and location of the data and log files.
6. The Management Group Name cannot be changed after installing MOM without removing all of the MOM components in that management group and reinstalling them. *The management group name is alphanumeric and must be unique.*
7. Specify the Data Access Service Account. Because the only component you are installing on Fountain is the MOM database, this is the only service account information that will be requested at this time.
8. On the MOM Error Reporting screen check the Enable Error Reporting Option and take the default of Automatically Send Reports to Microsoft.
9. For the Active Directory Configuration step, specify whether all the computers you will be managing are in domains that trust each other.

MOM Setup is now ready to begin the installation process.

Installing the Remaining Management Group Components To install the remaining management group components on the Monarch server, go through steps 2 and 3 of the installation overview—run the prerequisite checker for the remaining components and then run the installation wizard to install additional components. Follow these steps:

1. Check prerequisites, specifying the MOM 2005 Management Server as the component, as illustrated in Figure 6.13.

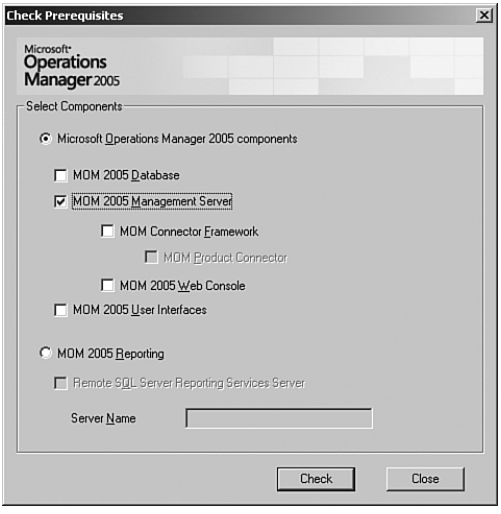


FIGURE 6.13 Check prerequisites for a MOM 2005 management server.

2. Initiate the MOM installation wizard, the second setup task on the setup menu.
3. Select Custom setup, and at the Custom Setup screen, make sure that the MOM 2005 Management Server and the MOM 2005 User Interfaces are selected, as shown in Figure 6.14.
4. You are asked to supply the location of the MOM database server instance because Setup could not find a database server on Monarch. Specify Fountain as the MOM database server and click Next, as illustrated in Figure 6.15.
5. Identify the Management Server Action and Data Access Server accounts. At this point, the wizard is ready to install the management server components. The remaining screens will be the same as they were in the "Single Server Configuration" section earlier in this chapter.

The installation process will now proceed.

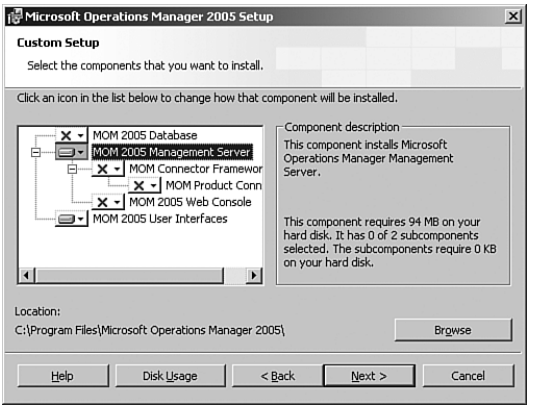


FIGURE 6.14 Custom setup for the management server and user interfaces.

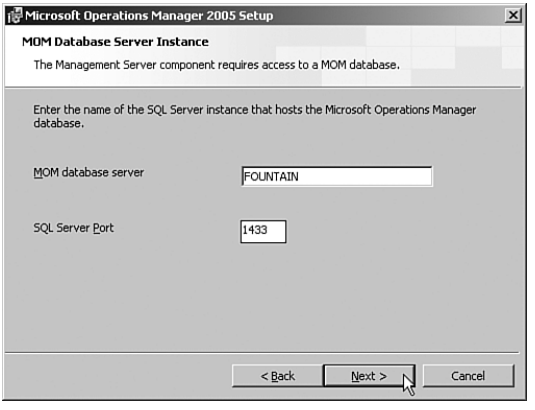


FIGURE 6.15 Specify the database server instance.

Installing Additional Components

Now that the required management server components are in place, you can use Setup to install additional components at any time. This could include installing consoles to servers other than the management server, installing the Web console, installing MOM Reporting, or installing the MOM Connector Framework (MCF). The MCF is covered in Chapter 19.

Installing the Web Console

You will use the Setup installation wizard to enable the Web console. The Web console requires that the Internet Information Services (IIS) Server component on the management server have the proper virtual directories created and loaded with the web pages and components to run the MOM Web console. Follow these steps to install the Web console:

1. When you run the MOM setup program on the management server, because you have already installed MOM components to this computer, you will be asked whether you want to modify, repair, or remove your installation. In this case, select Modify as shown in Figure 6.16.

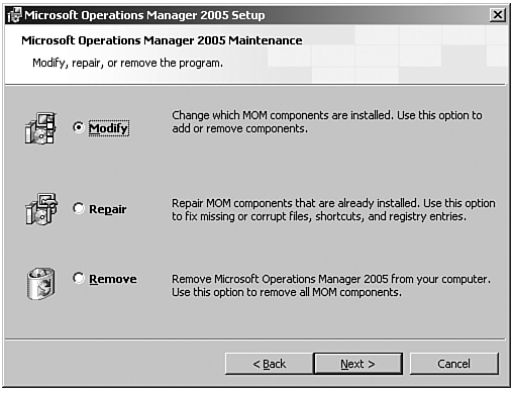


FIGURE 6.16 Select Modify to change which MOM components are installed on the management server.

2. At the Custom setup screen, make sure that for the MOM 2005 Management Server the MOM 2005 Web console is selected, as shown in Figure 6.17.

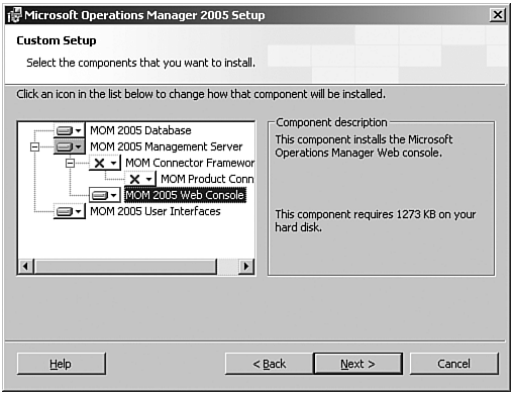


FIGURE 6.17 Specify the MOM 2005 Web console component.

Selecting Components

Because we are modifying an existing MOM installation, any previously installed components on that particular server are displayed as enabled. Select the additional components to install, but do not deselect any previously installed items or those components will be removed from the server!

3. Setup verifies that the applicable prerequisites are installed, and the wizard proceeds to install the selected component.

Installing the Reporting Server

Before you install MOM Reporting, SQL Server 2000 Reporting Services must be operational. Although the MOM Reporting portion of the setup is straightforward, SSRS installation may take a considerable amount of time.

Running SSRS Setup

The SSRS 2000 Setup cannot be run from a mapped drive to a network share. You can run the setup program from the installation media (CD-ROM), a local folder, or a file share referenced in Universal Naming Convention (UNC) format.

There are a number of caveats to the SSRS setup, which are documented in the setup help file (rssetup.chm) and readme file (readme_en.htm), both of which are located in the root directory of the SQL Server Reporting Services installation media.

- SSRS setup requires that the Microsoft Distributed Transaction Coordinator (MS DTC) service be available and that its Startup type be set to Automatic or Manual.
- The base version of SSRS 2000 requires connection to a SQL Server 2000 SP3a implementation; for MOM 2005 SP1 Reporting use SSRS 2000 SP1 (or a later version of maintenance) and SQL Server 2000 SP4.
- The default website must be accessible through http://<*servername*>.
- If you are running Windows Server 2003, the computer must be configured as an application server.
- If you are planning to use the Network Service account to run the ReportServer service, you must apply SQL Server QFE 859, which is also part of SQL Server 2000 SP4.
- The Report Manager requires a web server with ASP.NET.
- If you will be using Secure Sockets Layer (SSL) to secure the data on your reports, you must have an SSL certificate installed on your server and associated with the default website on the machine that will be hosting the report server, or the installation will fail.
- The SQL Server Agent service must run under a domain user account if you configure the report server to connect to SQL Server using a domain account and Windows authentication (versus using a SQL Server login or a built-in service account).

After installing SSRS on the SQL Server Reporting Services server, verify your SSRS installation by connecting to the reporting services website, http://<*servername*>/reports.

Installing MOM Reporting

After successful installation of SQL Server Reporting Services 2000 and any required prerequisites, move on to the MOM Reporting installation step. At the server you have designated as the MOM reporting server, run the Microsoft Operations Manager 2005 Setup program from the installation media to begin the setup process.

Running the Prerequisite Checker for MOM Reporting

Normally we recommend running the prerequisite checker prior to actually installing any MOM components, but if you run the check prerequisites for MOM Reporting using the slipstreamed version of MOM 2005 Service Pack 1, the utility gives you the error: "Unable to contact the Microsoft SQL Server Reporting Services server via Web Service" with an Unspecified error returned in the Recommended field of the report. This error is described in KB article 909846 (http://support.microsoft.com/kb/909846/).

As the report setup process also checks prerequisites, you can skip the standalone check if you have the slipstreamed version of MOM 2005 with SP1.

At the opening splash screen, select Install Microsoft Operations Manager 2005 Reporting, which is the third item on the Setup Tasks tab. To avoid any potential resource conflicts, be sure to close any other open programs running on your system. Follow these steps:

1. In the first few screens, you accept the license agreement, enter your user information, and specify the destination folder for the reporting software. You then specify the location where you installed SQL Server Reporting Services. Figure 6.18 shows the SQL Server Reporting Services Server screen.

   If the SSRS computer is on the other side of a firewall from the MOM reporting database server, clear the Automatically Detect Virtual Directories check box and enter the URLs for the virtual directories.

FIGURE 6.18 Enter the SQL Server Reporting Services Server name.

2. The prerequisite checker now automatically verifies the hardware and software requirements. Unlike the standalone version of the utility, the prerequisite checker will run successfully in a slipstreamed MOM 2005 SP1 setup when there are no outstanding issues. If errors are returned, implement the resolutions given in the report output from the prerequisite checker and rerun the installation step.
3. As shown in Figure 6.19, specify the location of the MOM database server instance. If the OnePoint database is installed in the default instance, you need only specify the server name; otherwise, specify the computer name and instance name. Our example shows that OnePoint is installed in the default instance on Monarch.

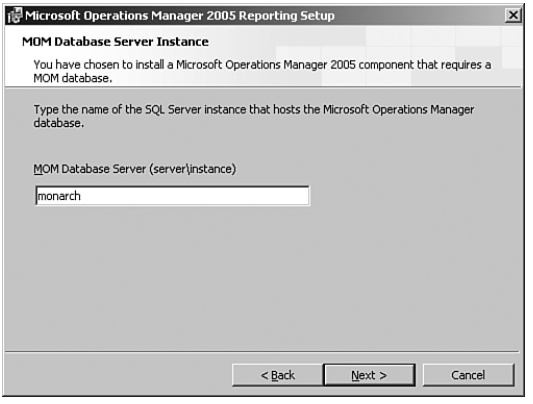


FIGURE 6.19 Enter the MOM database server instance.

4. The next screen looks similar to that shown in Figure 6.19, except that you enter the name of the local SQL Server instance that will host the MOM reporting database. This can be the SQL Server instance used with the SQL Server Reporting Services installation or a separate server.
5. You now proceed to the Database and Log File Information screen, illustrated in Figure 6.20, where you enter the size and location for the data and log files to be used by MOM Reporting. The default size is 1,000MB.
6. The data transfer task account runs the scheduled task, transferring data between the MOM database and the MOM reporting database. This should be a domain account if the two databases are on separate computers. In Figure 6.21, you are asked to specify this account and its credentials.

Specifying the Data Transfer Task Account

Consider using the DAS account because it already has the necessary permissions.

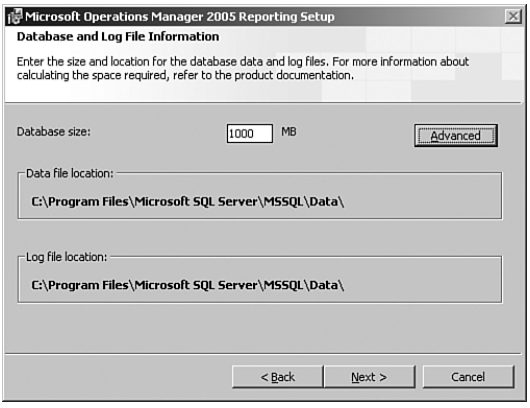


FIGURE 6.20 Specify database and log file information.

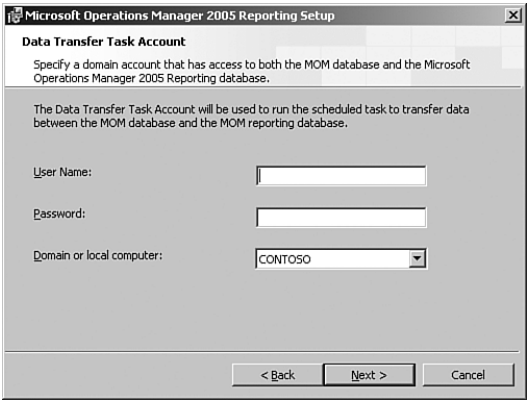


FIGURE 6.21 Enter the Data Transfer Task account.

7. Specify the account SQL Server Reporting Services will use to connect to the MOM reporting database.

   If SQL Server Reporting Services and the MOM reporting database are on the same computer, the Reporting User account can be a local account. If you are using separate computers, the account must be a domain account with access to the MOM reporting database. Enter the information requested in Figure 6.22.

8. On the Operational Data Reports Settings page, select the Yes, I Want to Send Operational Reports option if you want MOM to automatically send operational data reports to Microsoft. This setting is recommended.

9. Now you are at the Ready to Install page! Click Install to begin the installation process.

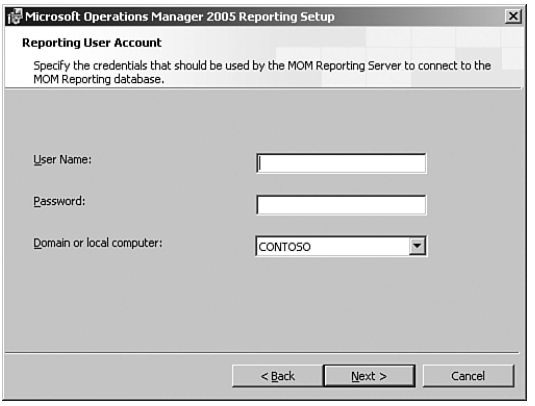


FIGURE 6.22 Specify Reporting User account credentials.

10. The last page of the wizard tells you that MOM Reporting has been successfully installed. Select the check box to Transfer Data from the MOM Database Now (see Figure 6.23), which verifies your MOM Reporting installation.

    MOM runs a scheduled task to transfer data from the MOM database to the MOM reporting database. By default, this task runs at 1:00 a.m. each day.

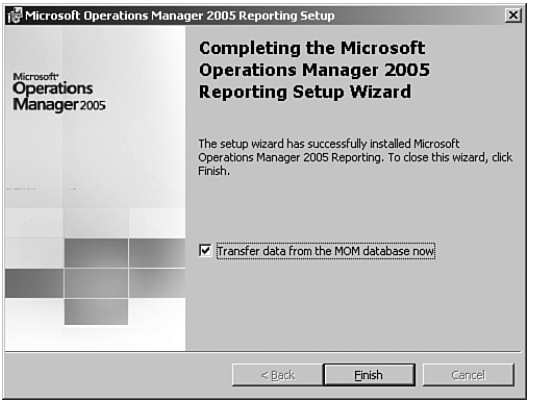


FIGURE 6.23 Transfer data from the MOM database now.

Congratulations! You have completed your MOM 2005 installation. Opening the Operator console without errors will confirm that you have installed MOM successfully.

Moving the Reporting Database

The supported way to move the reporting DB to a new machine is to uninstall MOM Reporting and then reinstall it on the new machine. Microsoft knowledge base article 922332 (http://support.microsoft.com/kb/92232/) explains the process, including

exporting reports from the original server and loading them to the database on the new machine.

Alternatively, to keep your old reporting data you can detach the SystemCenterReporting DB from the old system (after uninstalling MOM Reporting because the uninstall process does not delete the database), detach the database with the same name from the new machine and delete it, copy the old one to the new machine, and attach it.

MOM 2005 with SQL Server 2005 Implementation Steps

The following process can be used to install MOM 2005 using SQL Server 2005 as your database engine:

1. Install SQL 2005 on the database server(s). You should also install the SQL Server Management Studio unless you will be remotely managing your database installation.
2. Install MOM 2005, checking prerequisites first. You can start the Operator console to verify that all is well with MOM.
3. Install SQL 2005 Reporting.
4. Microsoft provides three hotfixes required when using SQL Server 2005. Knowledge base articles are available describing each of these hotfixes:
   - KB913812, at http://support.microsoft.com/kb/913812/
   - KB915785, at http://support.microsoft.com/kb/915785/
   - KB913801, at http://support.microsoft.com/kb/913801/
5. Install MOM 2005 Reporting Services.
6. To verify your Reporting Services installation, open up Scheduled Tasks and run the SystemCenterDTSPackageTask. If it completes with no errors in the Application log, you are now in business!

Detailed information on a SQL 2005 MOM installation experience can be found at http://ddmont.blogspot.com/2006_03_01_ddmont_archive.html. You can also see Andy Dominec's article in his blog on Techforum at http://myitforum.com/cs2/blogs/adominey/archive/2006/04/06/19671.aspx. Microsoft knowledge base article 918481 (http://support.microsoft.com/kb/918481/) describes the prescribed steps.

Troubleshooting Tips

MOM 2005's installation process includes an excellent prerequisite checker, which forestalls a number of problems. However, problems can crop up during the installation; the most common problems encountered relate to the reporting services components rather than the MOM components.

This section discusses some common problems that can occur during installation and how to work around them.

SQL Server Reporting Services Activation Problem

If you have problems with the reporting services setup on Windows Server 2003, where the setup completes successfully but gives you the following error:

Setup could not initialize the report server.

```
You must manually initialize the report server before using it for the first time.
```

Everything looks okay, except for an error in the RS log:

```
ACTIVATIONFAILED = 1.
```

Check IIS access to a test web page by creating a web page in the default IIS directory called test.htm page. If the page fails to load properly, it means that IIS is not functioning properly. A common problem is mismatched or incompatible DLLs, which can be resolved by reapplying Windows Server 2003 SP1.

This problem comes up almost always where a Windows Server 2003 system was installed using RTM media, SP1 was applied, and then IIS services are loaded (with the attendant swapping of the Windows Server 2003 RTM and Windows Server 2003 SP1 CDs). Something happens with the DLLs, and they are not correctly installed. Reloading Windows Server 2003 SP1 resolves the mismatched DLL errors.

Installing MOM 2005 on SQL Server 2000 SP4

When installing the MOM 2005 Released to Manufacturing version (RTM) management server or database onto a SQL Server 2000 SP4 system, the installer will fail because it expects SQL Server 2000 SP3. MOM 2005 SP1 supports SQL 2000 SP4, and we highly recommend using the full service pack release as an alternative because SP1 also fixes other issues found in the RTM release of the product, particularly if you are running SP1 of Windows Server 2003.

If you must install the RTM version of MOM 2005, the workaround is to change the SQL version registry value on the database server to trick the MOM 2005 RTM install into thinking that it is an older version. The registry key in question is the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\MSSQLServer\CurrentVersion. Find the CSDVersion value and change it from 8.00.2039 to 8.00.761 (assuming that you have SQL 2000 SP4). Then install MOM 2005. After the installation completes, change the value back to 8.00.2039.

This is a workaround only if you use the MOM 2005 RTM media. If you have the MOM 2005 SP1 media, this workaround is not necessary. Another alternative would be to bypass the prerequisite checker during the installation phase. Information regarding this is available at http://support.microsoft.com/kb/902803/.

MOM 2005 Reporting Server and Windows 2003 Service Pack 1

Sometimes there can be a problem installing the MOM 2005 reporting server. The situation occurs in a system with Windows 2003 SP1, SQL Server 2000 SP3a, MOM 2005 SP1, and SQL Server 2000 Reporting Services. When installing the MOM reporting server component, the following error occurs:

```
Failed to create data source for data warehouse.  An exception occurred.  Check
that you can access the SQL Services Reporting Server from this machine.  Error
code: -2147467259
```

Windows Server 2003 SP1 includes a loopback check security feature designed to help prevent reflection attacks on the computer. The check causes authentication to fail if the Fully Qualified Domain Name (FQDN) does not match the local computer name.

To solve this issue, you must disable the loopback check feature. To disable the loopback check, follow these steps:

1. Click Start, click Run, type **regedit**, and then click OK.
2. In Registry Editor, locate and then click the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa.
3. Right-click Lsa, point to New, and then click DWORD Value.
4. Type **DisableLoopbackCheck** and then press Enter.
5. Right-click DisableLoopbackCheck and then click Modify.
6. In the Value data box, type **1**, and then click OK.
7. Quit Registry Editor and then restart your computer.

After performing the preceding changes, MOM Reporting Service should install correctly.

DCOM Permission Problem

There is an undocumented incompatibility of installing MOM Reporting onto a system running Windows Server 2003 SP1. The Windows Server 2003 Service Pack 1 slightly alters the way DCOM works and its permissions. Unfortunately, MOM does not give you a descriptive error, displaying the following information:

```
Unable to contact the Microsoft SQL Server Reporting Services server via Web
Service.
```

In addition to completing the standard DisableLoopbackCheck registry hack described previously, you must also go into the DCOM configuration and change the permissions. Do the following:

1. From a command line, open DCOMCnfg.exe.
2. When it opens, expand Component Services and then Computers.
3. Right-click on My Computer and select Properties.
4. Choose the COM Security tab.
5. Under Launch and Activation Permissions, click Edit Default.
6. There you need to add the account you installed MOM under and the local groups of MOM Users and MOM Administrators.
7. Give all those accounts full allow privileges (local launch, remote launch, local activation, remote activation) and reboot.

It is possible that a normal installation through the GUI will still fail. Microsoft recommends a command-line installation in the following manner: `msiexec /i MOMReporting.msi /l*v installlog.txt`. Monitor the log file to ensure that the installation was successful.

Installation Errors

Table 6.7 describes some of the potential errors that might occur when installing MOM 2005. The knowledge base article number can be used to get more detailed information in the Microsoft knowledge database at http://support.microsoft.com.

TABLE 6.7 Potential Installation Errors

Process Erroring	Error Message	Potential Cause	Knowledge Base Article Number
2005 Install	"Failed to create MOM database" error when you try to install MOM 2005 on a computer that has been upgraded to Windows Server 2003.	When you upgrade to Windows Server 2003, the version of the Oledb32.dll file located in both the WINNT\System32\Dllcache folder and the Program Files\Common Files\System\Ole DB\Oledb32.dll folder on the Windows 2000–based computer is not upgraded to the version of the Oledb32.dll file included in Microsoft Data Access Components (MDAC) 2.8.	885734

Process Erroring	Error Message	Potential Cause	Knowledge Base Article Number
2005 Install	Event ID: 9122 appears in the Application log and agents cannot communicate with the management server after you install MOM 2005	This problem occurs if you have a NETBIOS domain name that contains a period.	889187
2005 Install	You receive a "The computer name has changed after SQL Server was installed" error message when you install Microsoft Operations Manager 2005.	Computer was renamed after SQL Server was installed but the SQL Server was not renamed.	899159
2005 Install	You receive a "Microsoft SQL Server 2000 SP3a or above required" error message when you try to install MOM 2005.	You are trying to install MOM 2005 on a computer that has SQL Server Service Pack 4 installed.	902803
2005 Install	When you try to install a MOM 2005 management server, the error is "Database Not Found" and the Next button in the installation wizard is dimmed.	There are no jobs whose names start with "OnePoint" in the Sysjobs table.	904744
2005 Install	Various	Describes a number of errors with resolutions when installingMOM 2005.	920215
2005 Reporting Install	You receive a "Microsoft SQL Server Reporting Services is not installed" error message when you try to install MOM Reporting.	One of the following: You specified an incorrect or an unavailable computer name or instance of SQL Server when you installed MOM 2005 Reporting. You are running a beta release of SQL Server Reporting Services. The SQL Server Reporting Services installation is incomplete or is corrupted.	883326

TABLE 6.7 Continued

Process Erroring	Error Message	Potential Cause	Knowledge Base Article Number
2005 Install or 2005 Reporting Install	Error 2755 in the MOMServer.log when you try to install Microsoft Operations Manager 2005 or MOM 2005 Reporting.	One of the following: You try to install MOM 2005 from a mapped network drive. You try to install MOM 2005 during a Terminal Services session. You try to install MOM 2005 from a UNC session to the MOM 2005 CD.	883328
2005 Reporting Install	You receive an "Unable to contact the Microsoft SQL Server Reporting Services server via Web Service" error message when you try to install MOM 2005 Reporting.	One of the following: You are installing MOM 2005 SP1 using a slip streamed version of MOM 2005 SP1, and you are running the prerequisite checker. You try to install MOM over a Secure Sockets Layer (SSL) connection.	909846 and 899720; workaround provided in articles
2005 Reporting Install	You may receive an "Incorrect version of Microsoft SQL Server Reporting Services is installed" error message when you try to install MOM 2005 Reporting.	You are trying to install MOM 2005 Reporting on a computer where Microsoft SQL Server 2000 Reporting Services Service Pack 2 is installed.	902804
2005 Reporting Install	You receive a "Could not get SQL Server instance names" error message when you try to install MOM 2005 Reporting.	One of the following: You try to install MOM Reporting from a remote system. You do not have service pack 3a or later of SQL Server 2000 installed.	911681

Process Erroring	Error Message	Potential Cause	Knowledge Base Article Number
2005 Reporting Install	You receive a "Failed to create data source for Data Warehouse. An exception occurred. Check that you can access the SQL Services Reporting Server from this machine. Error code: -2147467259 (Unspecified error)" message when you try to install MOM 2005 Reporting.	Windows Server 2003 SP1 security enhancements, which include a loopback check security feature that designed to help prevent is reflection attacks on the computer.	917664; workaround provided in article
2005 Reporting Install	Various	Describes a number of errors the prerequisite checker encountered when checker encountered when trying to install MOM Reporting. Also contains links to individual KB articles.	919954
2005 Reporting Install	Installation fails when you try to install MOM 2005 Reporting on a computer running Microsoft SQL Server 2005.	One of the following conditions is true: You try to install MOM 2005 Reporting on a computer that is running a 32-bit version of Microsoft SQL Server 2005. The 32-bit version of SQL Server 2005 is running on a cluster based on a 64-bit version of Microsoft Windows Server 2003. You do not provide the full Microsoft Windows Installer path in the command line.	922337

Summary

This chapter discussed the hardware and software prerequisites and requirements for MOM 2005. We went through two installation scenarios and processes: for a simple environment where all of the MOM components are on the same server and a more common

production system scenario where the database component is on a separate server from the management server. We also discussed the process to install optional components including the Web console and MOM Reporting.

The next chapter covers what you need to know to upgrade or migrate to MOM 2005 if you already have an earlier version of MOM in your environment or are running MOM 2005 Workgroup Edition.

CHAPTER 7

Upgrading to MOM 2005

IN THIS CHAPTER

If you already are using Microsoft Operations Manager (MOM) and are planning on upgrading to MOM 2005, you have come to the right place! This chapter discusses the steps required to upgrade from an existing MOM environment, such as MOM 2000 SP1 or MOM 2005 WorkGroup Edition, to MOM 2005. We also review planning and security considerations for deploying MOM 2005.

Planning Your Upgrade

Before starting the upgrade process, you will need to plan your MOM implementation. As discussed in Chapter 4, "Planning Your MOM Deployment," prior to upgrading MOM 2005 you should assess, design, plan, and test the process within a proof of concept (POC) environment.

Part of your assessment should include identifying the servers that currently provide MOM services. The specific server configuration used by your organization determines which steps will be required for your upgrade and the complexity of the upgrade. If all MOM components are on a single server, the upgrade is far simpler than if there are multiple DCAM servers, administrator consoles, or a clustered SQL backend. If you are not familiar with the details of your current MOM configuration *Do Not Pass Go*—return to Chapter 4.

The upgrade from MOM 2000 or MOM 2005 Workgroup Edition to MOM 2005 has some important qualifications to keep in mind. It is important to note that MOM 2000 agents are not supported in MOM 2005, although they can continue to run in a MOM 2005 management group during the upgrade process. Nor is there support for installing

MOM 2000 SP1 agents after the MOM environment is upgraded to MOM 2005. Additionally, MOM 2005 does not support MOM agents installed on Windows NT 4.0 systems. If these servers still require monitoring after your MOM 2005 upgrade, the MOM 2000 agents must be uninstalled, and these computers monitored as agentless managed computers.

If your environment is using MOM 2005 Workgroup Edition, the upgrade process is straightforward because MOM 2005 Workgroup Edition supports only a single-server configuration.

Before delving into the process of upgrading your MOM environment, we will discuss security and considerations for the impact to the online help files during the upgrade.

Security Considerations

Significant security changes have occurred comparing MOM 2000 SP1 to MOM 2005. Although MOM security is discussed in detail in Chapter 11, "Securing MOM," changes that impact security during the upgrade process are discussed here. These changes relate to service account and authentication changes within MOM.

Service Accounts

The first major change in security is related to the splitting of the MOM 2000 DCAM components (which use two service accounts: the DAS account and the Consolidator and Agent Manager account) into three separate accounts: the MOM Service account, the Management Server Action account, and the DAS account. This change enables you to increase security by utilizing lower privileged security accounts. The MOM 2005 accounts and their required permissions are

- MOM Service account—This account is used for communication between the agents and the management server. By default the account uses the credentials of either Local System or Network Service (available with Windows 2003). The MOM service is responsible for communication between the agents and the management server.
- Management Server Action account—This account must be a domain account and must also be a member of the local Administrators group on the management server. If you want to utilize "automatic agent management" the account must also have administrative rights on each server where MOM will run an agent.
- DAS account—The DAS account requires database owner access to the MOM database, OnePoint, which is granted during the database installation.

Security Considerations for the Management Server Action Account

The Management Server Action account could be added to the Domain Admins group although that approach greatly decreases the effective security of MOM 2005 and is not recommended by Microsoft. Because a domain administrator is a member of the local Administrators group on every computer in the domain, this account would have administrative privileges on machines not monitored by MOM.

Mutual Authentication

Another security enhancement to be considered when upgrading from MOM 2000 is *mutual authentication*, which means that the management server and the agent will authenticate each other before communication occurs. Mutual authentication is disabled by default during the upgrade process from MOM 2000 SP1.

Using Mutual Authentication

The configuration of mutual authentication should be reassessed after the MOM 2005 migration is complete. Mutual authentication is discussed in detail in Chapter 11.

When implementing mutual authentication, a second configuration option is available; this is a check box labeled Block MOM 2000 and MOM 2000 SP1 Agents from Connecting to the Management Server. This choice is not available unless mutual authentication is selected and is disabled by default while MOM 2000 SP1 is upgraded to MOM 2005. These two settings can be modified during the setup process but should not be changed until all agents are upgraded. The settings are configured within the Global Settings section of the MOM 2005 Administrator console. If mutual authentication is enabled, MOM 2000 SP1 clients cannot communicate with the management server, so make sure that this setting is disabled if you require communication with MOM 2000 SP1 clients. Disable this setting when transitioning from MOM 2000 to MOM 2005 or in multihomed configurations where one MOM environment is MOM 2000 and the other is MOM 2005.

Help File Considerations

The online help within MOM 2005 is installed as part of the upgrade process from MOM 2000 and is accessible from the MOM 2005 Administrator and Operator consoles. When the MOM 2000 DCAM servers are upgraded to MOM 2005 management servers the existing MOM 2000 help files will be removed, and new help files for MOM 2005 will take their place.

Using Both Versions of the Help Files

If you will have a mixed environment, as when there are MOM 2000 agents reporting to the MOM 2005 server, you may still need access to MOM 2000 help. The MOM 2000 help file can be found on the MOM 2005 installation CD under the pfiles\mom2005\help directory structure. You should only need these files if you are performing a mutihomed migration, as discussed in the "Side-by-Side Migration" section later in this chapter.

Upgrading MOM 2000 SP1

This section discusses an overview of the upgrade process, describes sample upgrade scenarios, and provides the steps to perform the upgrade of your environment from MOM 2000 SP1 to MOM 2005.

Upgrade Overview

The general process involved in upgrading from MOM 2000 SP1 to MOM 2005 is the same regardless of the complexity of the configuration being upgraded. Each of the following steps is discussed in detail in the "MOM 2000 Upgrade Detailed Steps" section later in this chapter. The basic steps required are as follows:

1. Verify upgrade path. Verify that your current environment is on the supported upgrade path list. It is important to understand that an upgrade from MOM 2000 without MOM 2000 SP1 applied is not supported.
2. Back up MOM 2000. Back up your current MOM 2000 SP1 OnePoint database and export any custom management packs.

Always BACK UP!

The one time that you don't have a backup is the one time that you will need the backup. This is our personal version of Murphy's Law.

3. Upgrade consoles first. MOM 2000 allowed you to install a MOM Administrator console on a server that was not a DCAM or database server. If you have one or more administrator consoles installed on non-MOM servers you should upgrade them to MOM 2005 now. Do not upgrade consoles on the DCAM server at this point; wait to upgrade the DCAM servers after the database upgrade is complete.

Console Behavior on Remote Machines

The MOM 2005 Operator console will not function until the DCAM is upgraded to a MOM 2005 management server. The MOM 2005 Administrator console will behave like a MOM 2000 console when it is connected to a MOM 2000 DCAM.

4. Upgrade MOM database server. MOM 2000 also supported a configuration where you could install the OnePoint database on a separate machine from your DCAM servers. If your environment currently has the SQL Server database running on a different server (including on a cluster), upgrade it now.
5. Upgrade MOM DCAMs. After the consoles and the database server have been upgraded you will upgrade the MOM 2000 DCAM(s).
6. Upgrade agents. As each of the DCAMs in your MOM 2000 SP1 environment is upgraded to MOM 2005, upgrade the agents on the servers monitored by that DCAM.
7. Remove MOM 2000 Reporting. The reporting functionality has been completely replaced in MOM 2005. The upgrade process, however, does not automatically remove MOM 2000 Reporting. You should uninstall the original MOM 2000 Reporting using the add/remove programs component in Windows.

8. Import management packs. Finally, after you have completed the first seven steps it is now time to import management packs into the MOM 2005 environment. The latest versions of MOM management packs are available from the Microsoft Management Pack Catalog at http://go.microsoft.com/fwlink/?linkid=43970.

Follow the Upgrade Steps in Their Specified Order

It is suggested that you exactly follow the steps of the preceding upgrade process identified because deviation can lead to unexpected results. By way of example, if you add management packs before upgrading all DCAMs, the non-upgraded DCAMs would then receive unnecessary alerts and events.

Upgrade Scenarios

Although the previous eight general steps apply to any upgrade process, your environment's configuration determines the specific details required for your upgrade. To provide an upgrade path that most closely matches your own environment, we have created several possible scenarios that illustrate the types of changes that need to be made for specific upgrades. Each scenario is available for your review but feel free to go directly to the scenario that most closely matches your current environment. The scenarios include

- Single server upgrade—Use this one if your MOM 2000 SP1 environment uses a single physical server for all MOM server functions including the MOM database, console, and DCAM.
- Single server with separate MOM console(s)—In this example your MOM 2000 environment has a single server with the MOM DCAM server and database installed, but additional MOM console(s) exist on separate servers.
- Single DCAM server with separate MOM database server(s)—This scenario splits the MOM server functions between a MOM DCAM server and a MOM database server.
- Multiple DCAMs—If you have a MOM 2000 environment with multiple DCAM servers this section is for you.
- Side-by-side migration—You may want to consider this type of upgrade for complex and unique systems (or just to perform a fresh installation of MOM). The side-by-side migration leaves your existing MOM monitoring in place and allows your agents to report to both MOM 2000 and MOM 2005, providing additional time for you to switch to the new system. This type of upgrade also provides an opportunity to replace hardware running your MOM 2000 environment because the system(s) may be nearly at end of life.

Multitiered and Multihomed MOM 2000 Configurations

If your existing environment is multitiered or multihomed, Microsoft provides details on the upgrade process as part of the MOM 2005 Deployment Guide at http://go.microsoft.com/fwlink/?linkid=33535, and can also be downloaded from Microsoft's download center, http://www.microsoft.com/downloads/.

If your specific MOM configuration is not listed, don't worry; the "MOM 2000 Upgrade Detailed Steps" section later in this chapter discusses a process that applies to all MOM 2000 upgrades, regardless of your configuration.

Single Server Upgrade

For the single server upgrade we have one MOM server named Monarch with all MOM 2000 SP1 components running. Monarch is a DCAM database server and provides the only Administrator console for the environment.

Using our fictitious company, Contoso, as an example, assume that it has a single MOM Server installed that provides all MOM 2000 components, as illustrated in Figure 7.1.

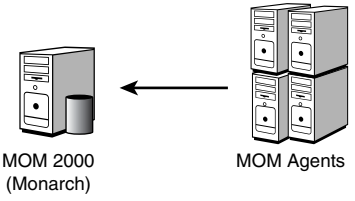


FIGURE 7.1 Monarch runs all MOM 2000 components—the DCAM, database server, and Administrator console.

For this configuration, you would perform the MOM 2000 SP1 verify, backup, DCAM, agents, uninstall MOM 2000 Reporting, and import management pack steps. The separate console and database upgrade processes are not required because there are no separate MOM consoles and the database services are running on the DCAM. The steps for each of these processes are discussed in the "MOM 2000 Upgrade Detailed Steps" section of this chapter.

Separate MOM Consoles

In this example we will upgrade a two-server configuration with all MOM 2000 SP1 components running on a server named Monarch and an additional Administrator console installed on a server named Cortez. Monarch is the DCAM and database server, and provides one of the Administrator consoles for the environment. Cortez only provides a separate MOM 2000 SP1 Administrator console. Figure 7.2 displays the MOM 2000 architecture including the Monarch and Cortez servers discussed previously.

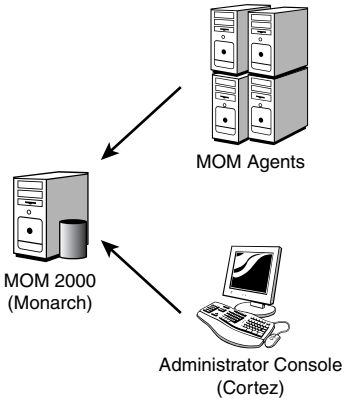


FIGURE 7.2 Monarch is the DCAM, database server, and Administrator console; a second server (Cortez) provides another Administrator console.

For this configuration, you would perform the MOM 2000 SP1 verify, backup, console, DCAM, agents, uninstall MOM 2000 Reporting, and import management pack steps described in this chapter. The database upgrade processes would not be required because database services are running on the DCAM, and the database will automatically be upgraded as part of the DCAM upgrade. The detailed steps for each of these processes are discussed in the "MOM 2000 Upgrade Detailed Steps" section of this chapter.

Separate MOM Database Server

For this example, we will consider a two-server configuration with all MOM 2000 SP1 components running on a server named Monarch with the exception of the MOM database server, which is running on Fountain. Monarch is a DCAM and provides the only Administrator console for the environment. Fountain is a single server (nonclustered) that processes the MOM 2000 SP1 database services. Figure 7.3 displays the MOM 2000 architecture including the Monarch and Fountain servers described previously.

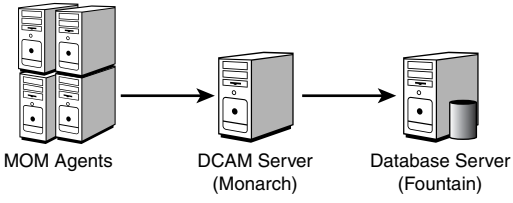


FIGURE 7.3 Monarch runs all MOM 2000 components while Fountain provides the database for the MOM environment.

In this multiple server MOM 2000 SP1 configuration you would perform the MOM 2000 SP1 verify, backup, DCAM, database, agents, uninstall MOM 2000 Reporting, and import management pack steps. The console upgrade processes would not be required because no

separate Administrator consoles exist. The detailed steps for each of these processes are discussed in the "MOM 2000 Upgrade Detailed Steps" section of this chapter.

Multiple DCAMs

For this example, we consider a two-server configuration with all MOM 2000 SP1 components running on Monarch and an additional MOM DCAM on a server named Keystone. Monarch and Keystone both provide DCAMs for the environment, and Monarch provides the MOM 2000 SP1 database services. Figure 7.4 displays the MOM 2000 architecture including the Monarch and Keystone servers discussed previously.

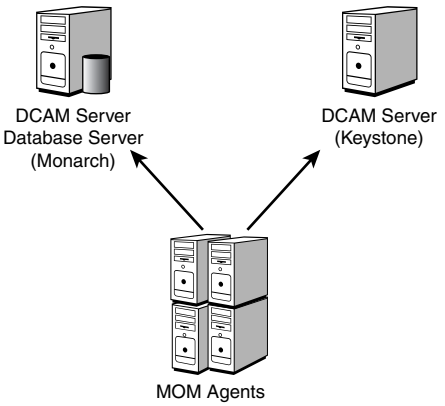


FIGURE 7.4 Monarch runs all MOM 2000 components while a second server named Keystone provides a redundant DCAM.

In this multiple server MOM 2000 SP1 configuration you would perform the MOM 2000 SP1 verify, backup, DCAM, database, agents, uninstall MOM 2000 Reporting, and import management pack steps. The console upgrade processes would not be required because there are no separate Administrator consoles. The first DCAM (Monarch), which has a database server would be upgraded first as part of the database upgrade process. The detailed steps for each of these processes are discussed in the "MOM 2000 Upgrade Detailed Steps" section of this chapter.

Side-by-Side Migration

The majority of this chapter discusses an upgrade approach to migration of your MOM 2000 environment. An alternative upgrade scenario is a multihomed or side-by-side upgrade process. Multihoming is a reasonable upgrade approach when your environment has significant customizations and processes built around your existing MOM 2000 SP1 configuration. The upgrade process by itself turns off your MOM 2000 monitoring and switches to MOM 2005 monitoring without first checking it against your production environment.

To enable overlapping monitoring during the testing phase, you can implement a multihoming upgrade scenario using both MOM 2000 SP1 and MOM 2005. By using multihoming, your existing MOM 2000 SP1 configuration group and a new MOM 2005 management group can monitor the same servers simultaneously. During this period, you can compare the monitoring scenarios between the two versions of MOM to verify that the new MOM 2005 management packs are monitoring the same data points that your MOM 2000 environment is set up to monitor.

This coexistence period also provides time to port any customizations that you have made into the new management groups. These customizations could include management packs, tools built on the MOM SDK, or external processes. This overlapping period could also be used as training time for support personnel who use MOM as a part of their jobs.

As part of the migration process, the MOM 2000 SP1 agents are upgraded to MOM 2005 agents—meaning that the MOM 2000 SP1 configuration group is communicating with and managing MOM 2005 agents. Both the MOM 2000 DCAM and the MOM 2005 agent are designed to support this scenario, with one additional configuration step. On the MOM 2005 installation media, in the Upgrade Tools directory, there is a management pack called MicrosoftOperationsManagerTransition.akm. This management pack provides the capability for MOM 2000 SP1 DCAMs to monitor MOM 2005 agents.

Using the MOM Transition Management Pack

The MOM Transition management pack is to be imported only into MOM 2000 SP1 configuration groups. Importing into a MOM 2005 management group can cause degradation when monitoring MOM 2005 agents.

The process for setting up this scenario is as follows:

1. Install a MOM 2005 management group. Do this on separate hardware from that used for your existing MOM 2000 SP1 configuration group. Refer to Chapter 6, "Installing MOM 2005," for the process to install a new MOM 2005 environment, which includes establishing a new management group.
2. Import the MOM Transition management pack into your MOM 2000 SP1 configuration group. This only needs to be done on one DCAM even if multiple DCAMS are in the configuration group.
3. Monitor servers from the MOM 2005 management group. This can be done using any of the standard ways of installing agents (the Install Agents Wizard, creating Computer Discovery rules, or performing manual agent installs). See Chapter 5, "Planning Complex Configurations," for agent installation details.
4. Import additional management packs into the MOM 2005 management group. Installing management packs into this configuration provides an environment for verifying that the new MOM 2005 management packs provide at least the same (in most cases, a much higher) level of coverage of the monitored applications.

After these steps are complete and you are satisfied with the monitoring of MOM 2005, you can deal with your legacy MOM 2000 SP1 configuration group and its hardware as you see fit: Either upgrade your configuration group to MOM 2005 following the steps in this chapter or retire the MOM 2000 SP1 environment.

Retiring a MOM 2000 Configuration Group

If you retire the MOM 2000 SP1 configuration group, convert all the managed computers to Unmanaged before turning off the hardware or uninstalling MOM. If you do not do this, the agent will continue to try to talk to the legacy configuration group. The recommended approach to convert managed computers to Unmanaged is to uninstall the agent from the MOM 2000 Administrator console. The other possibility, and the only option if the MOM 2000 servers are already retired, is to go to each managed server and modify the agent installation (through Add/Remove Programs) to remove the MOM 2000 configuration group from the agent.

MOM 2000 Upgrade Detailed Steps

In the previous sections we have discussed high-level approaches to migrations. This section focuses on the detailed steps associated with the upgrade process from MOM 2000 SP1 to MOM 2005.

Verify

Verify that your current MOM 2000 environment is on the supported upgrade path list given in Table 7.1.

TABLE 7.1 Supported and Nonsupported Upgrade Paths

Original Platform	MOM 2005 Base	MOM 2005 SP1
MOM 2000	No	No
MOM 2000 SP1	Yes	Yes
MOM 2000 SP1 Express	No	No
MOM 2000 SP1 Evaluation	No	No
MOM 2000 SP1 using MSDE	No	No
MOM 2005 Beta 3	No	No
MOM 2005 Release Candidate	Yes	No
MOM 2005 using SP1 update from the web	N/A	Yes
MOM 2005 using SP1 full version	N/A	No

Use MOM 2005 SP1

Although Table 7.1 shows both MOM 2005 base and MOM 2005 SP1 supported upgrade paths, we will assume for discussion purposes that you are using MOM 2005 Service Pack 1. MOM 2005 SP1 resolves a number of issues including those related to Windows 2003 SP1 support.

Real World—DCAM Configuration

Check the MOM 2000 SP1 configuration for each system listed under Agent Managers. Each DCAM should *not* have another DCAM listed as one of its managed computers. Each DCAM needs to specifically exclude the other DCAMs in the environment. *If one DCAM server has an agent deployed to another DCAM server, the installation process will fail when attempting to upgrade DCAMs.*

Backup

If the database server is either not being backed up currently or the backup process has not been tested, refer to article 325612 on the Microsoft support website for information on how to back up the MOM database server. Also, if you have custom management pack information you should export it for backup purposes. This article describes both the database server and the management pack export process and can be located at http://support.microsoft.com/kb/325612/.

Upgrade the Console

If your environment has MOM Administrator consoles installed on non-DCAM servers, these systems are upgraded before any other upgrades occur. The following steps are required to upgrade an existing MOM 2000 Administrator console to MOM 2005.

1. Be sure to close the MOM 2000 SP1 Administrator console before starting the setup process.
2. Run the MOM Setup program. You can run Setup from either the Microsoft Operations Manager 2005 CD or a shared network installation point. If you are using a CD-ROM, inserting the disk causes Setup to start automatically. If you are installing over the network, find and run setup.exe, which should be in the root of the MOM 2005 installation directory.

The MOM Setup Program

The MOM Setup program is also known as the Microsoft Operations Manager 2005 Setup Resources program.

3. Check prerequisites for the MOM 2005 user interface. If there are any warnings or errors, resolve them and rerun the Prerequisite Checker. Close the Prerequisite Checker to continue.
4. After resolving any prerequisite issues, on the main menu of the MOM setup choose the Install Microsoft Operations Manager 2005 option.
5. The first few screens of the installation wizard are fairly typical. You will accept the license agreement and enter user information and your product key.
6. If MOM 2000 Server components are detected, the Upgrade Microsoft Operations Manager screen is displayed. Click on the Upgrade to MOM 2005 button, accept or change the default installation location, and click Next to continue.

7. The setup program automatically runs the prerequisite check prior to actually beginning the upgrade. Resolve any errors from the prerequisite check and note any warnings to either resolve prior to or after the upgrade process. Click Next to continue.
8. Enter the name of the management server (use the name of the DCAM server, which in this example is *Monarch*). Click Next to continue.
9. Click Install to continue on the Ready to Install screen.
10. Click Finish to complete the installation on the Completing the Microsoft Operation Manager 2005 Setup Wizard screen (accept the checked box to start the MOM Administrator console).
11. You should be able to successfully start the Administrator console, which is providing data from the MOM 2000 SP1 environment. The Operator console will not function at this point in time and will error out connecting to the management server. The Operator console is new with MOM 2005, so the DCAM will need to be upgraded before remote Operator consoles can connect successfully to the management server.
12. Close out the Administrator console after verifying that it functions correctly.

Repeat this process for all additional Administrator consoles that are not installed on DCAM servers. After upgrading all Administrator consoles, proceed to the following "Upgrade the Database" section of this chapter.

Upgrade the Database

After you have upgraded your console server(s), the next step is to upgrade your database server. If your database server is running on a DCAM you should skip this step and proceed to the "Upgrade DCAM" section of this chapter. The DCAM upgrade process automatically upgrades the MOM database when both components are on the same server. The following steps are required to prepare the database for upgrade:

1. On the OnePoint database, check the DataFiles tab and verify that Automatically Grow File is not checked for the database. This configuration can stop the MOM database from functioning properly. If the Autogrow box is checked, uncheck it.

Problems When Using Autogrow

During automatic file growth all database operations are suspended, which can keep MOM from functioning properly. This is discussed in article #297778 on the Microsoft Support website at http://support.microsoft.com/kb/297778/.

2. You can never back up too many times. Before performing the upgrade, be sure to back up the database.

3. For the OnePoint database it is a best practice to groom the MOM Database before performing the upgrade process. Grooming the database speeds up the deployment process and decreases the initial data transfer process to the MOM 2005 reporting database. The procedure to groom the OnePoint database is described in article 298382 on the Microsoft support website at http://support.microsoft.com/kb/298382/.
4. Verify that the database size is within the recommended range, which is at least 300MB and a maximum of 30GB.

Database Sizing

The best practice approach is to maintain the database at between 12GB and 15GB. Verify that at least 40% of the total space is available as free space before starting the upgrade process.

5. In the MOM 2000 Administrator console, make sure that Auditing is turned off.

   To determine whether Auditing is turned off, open the MOM 2000 Administrator console. In the Navigation pane, go to Configuration \ Global Settings. In the Details pane right-click on the Auditing section and click on Properties. Check to make sure that the Audit Changes Made through the DAS on <*servername*> is unchecked for all servers listed. If it is checked, uncheck it. Click OK to exit the Configuration Group Global settings page.

Saving the Installation Log

For future debugging purposes, on the MOM database server, rename the *%ProgramFiles%*\Microsoft Operations Manager 2000\OperationsInstall.log file to Install.log (or any other nonexisting filename) in the same directory.

Database Agent Uninstallation

Do *not* attempt to uninstall the MOM 2000 SP1 agent from the database server using the add/remove programs applet. This can result in the removal of the database pieces of MOM and will create a nonfunctional MOM 2000 environment.

Change the DAS Account (Optional) It is recommended that you use the current DAS account when upgrading from MOM 2000 SP1 to MOM 2005. If that is not feasible for your environment, the following process changes the DAS account:

1. On the MOM 2000 SP1 DCAM, click Start, point to Programs, point to Administrative Tools, and then click Component Services.
2. Expand Component Services, expand Computers, expand My Computer, and then expand COM+ Applications.

3. Right-click on OnePointActiveOpsDas, and then click Properties.
4. On the Identity tab, enter the credentials for the new DAS account. The DAS account credential screen is shown in Figure 7.6 in the following "Database Upgrade" section of this chapter.

Database Upgrade After you prepare the database, uninstall the MOM agent, and address any DAS account issues, you can proceed to the actual upgrade of the database server. The following are the steps involved in upgrading the database server:

Upgrading Your Database in a Clustered Environment

If your external database server is running on a cluster, upgrade the primary node first and do not check the passive node box on the setup dialog. After this is completed, make the secondary node active and check the passive node box on the setup screen. Repeat the last step for each additional node.

1. Run the Microsoft Operations Manager 2005 Setup Resources program.
2. After resolving any prerequisite issues, on the main menu of the MOM setup choose the Install Microsoft Operations Manager 2005 option.
3. The first few screens of the installation wizard are fairly typical. You will accept the license agreement and enter user information and your product key.
4. When the MOM 2000 components are detected the screen displayed in Figure 7.5 appears. Click on the Upgrade to MOM 2005 check box and continue.

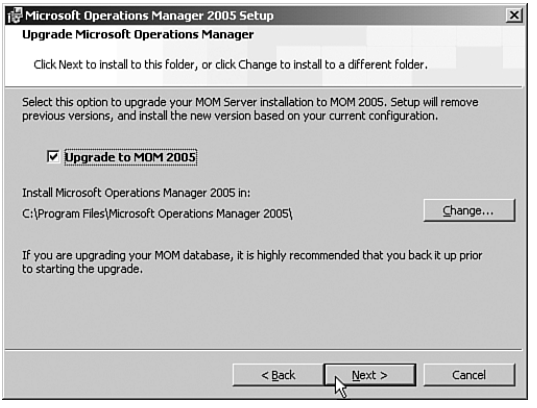


FIGURE 7.5 Check the upgrade option to upgrade the MOM 2000 environment.

5. At the prerequisite checking page, resolve any errors on the prerequisite checking page, and note any warnings to either resolve prior to or after the upgrade process.

6. Continue to the Data Access Server Account screen to enter your DAS Account username, password, and domain, as shown in Figure 7.6. This account requires database owner access permissions to the MOM database (OnePoint).

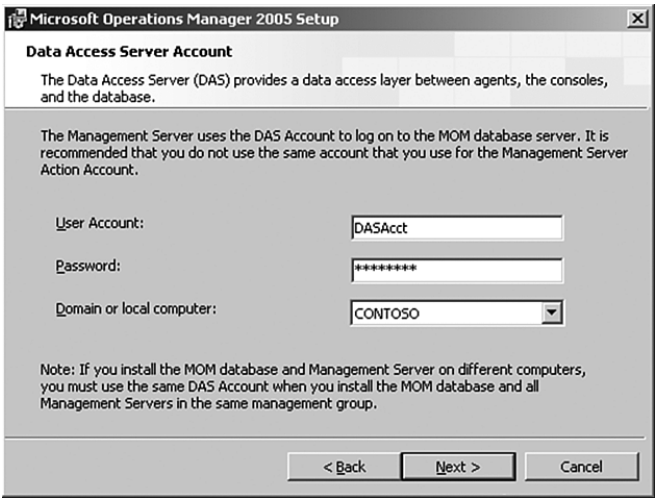


FIGURE 7.6 Enter user account, password, and domain for the Data Access Server account.

7. On the MOM Error Reporting screen check the Enable Error Reporting option and take the default of Automatically Send Reports to Microsoft.
8. Continue to the Ready to Install screen where you will click Next to continue.
9. Click Finish to complete the installation on the Completing the Microsoft Operation Manager 2005 Setup Wizard screen.

After you have successfully upgraded the database server or servers in your environment, you can proceed to the following "Upgrade DCAM" section of this chapter.

Upgrade DCAM

Now that we have upgraded any external consoles and the database server it is time to upgrade the DCAM servers in your environment. Your upgrade is in the home stretch at this point, so keep going! Follow these steps:

1. Be sure to close the MOM 2000 SP1 Administrator console before starting the setup process.
2. Run the Microsoft Operations Manager 2005 Setup Resources program.
3. Check prerequisites for the MOM 2005 management server.

4. Accept the defaults during the installation process. If you have questions on any of the installation screens, refer back to the "Upgrade the Console" and "Upgrade the Database" sections of this chapter.

5. On the Agent Action Account screen, specify your Agent Action account or take (subject to the following proviso) the default of Local System.

Agent Action Account

The Local System account should be used as the Action account except for circumstances where security is a paramount business requirement. Using a domain account as the Action account increases maintenance due to potential password changes and the need to grant specific permissions to the account.

If you are installing the MOM agent on Windows 2000 servers, the Action account must be a member of the local Administrators group or the Local System account. If you are installing the MOM agent onto Windows 2003 servers and do not use the Local System account, you should configure the Action account to have the following permissions:

- Member of the local Users group
- Member of the local Performance Monitor Users group
- "Manage auditing and security log" permission (SeSecurityPrivilege)
- "Allow log on locally permission" (SeInteractiveLogonRight)

Different management packs may require different levels of permissions, so be sure to review the management pack guides for details on additional required permissions.

If you will be using an account with limited privileges for the MOM Action account (versus an account that is a member of the domain administrators group), you can use group policies to provide the required permissions for the account(s).

6. Now enter your Data Access Server account username, password, and domain.

Security Requirements for the DAS Account

The Data Access Server account requires permissions onto the MOM database. The DAS account requires the "db_owner" role for the OnePoint database and SQL Server Security Login with Permit server access. The DAS account must also be a member of the SC DW DTS security groups on the MOM reporting server and MOM database server. The installation process will appropriately configure the DAS account you specify.

7. Click Finish to complete the installation on the Completing the Microsoft Operation Manager 2005 Setup Wizard screen (accepting the checked box to start the MOM Administrator console).

8. Validate that the Administrator console now shows that the full version of MOM 2005 is installed and verify that MOM agents are still reporting status correctly.

Repeat this process for all additional DCAM servers. After upgrading the DCAM server(s), you can move to the following "Upgrade Agents" section of the chapter.

Upgrade Agents

You have now upgraded all of the MOM 2000 SP1 servers to MOM 2005, so the next step is to upgrade the agents on the servers MOM 2000 SP1 was monitoring.

Pending Agent Upgrades Now that your DCAMs are upgraded, you can upgrade the agents that were remotely installed within your MOM 2000 environment. Perform the following steps:

1. In the MOM 2005 Administrator console, expand the Computers area, and then click on Pending Actions.
2. Right-click on the agent to upgrade and choose Install Agent Now. (You can also multiselect agents here to make the process faster.)
3. Continue to the Agent Installation Permissions screen, where you will choose an account that has at least local administrative permissions on the target computer(s).
4. At the Agent Installation Directory screen you can accept or change the default location of *%ProgramFiles%*\Microsoft Operations Manager 2005.
5. Go to the Completing the Agent Install Wizard screen and click Finish.

Finally, it is time to upgrade the agents that were manually installed in the MOM 2000 environment.

Manual Agent Upgrades To upgrade an agent that was installed manually in MOM 2000, perform the following steps:

1. Log in to the computer where the manual agent was installed.
2. Launch the agent installation from the Setup Wizard or run the MOMAgent.msi file available on the MOM 2005 CD under the \I386 directory for standard Intel based systems, and under the \IA64 directory for the 64-bit version of Windows. You can also create a share point for the \I386 directory on the MOM server under the installation directory for MOM 2005, which by default will be at *%ProgramFiles%*\Microsoft Operations Manager 2005.
3. Click Next on the Microsoft Operations Manager 2005 Agent Setup screen; then select the Upgrade to MOM 2005 Agent Now check box. Click Next to continue.
4. On the Ready to Modify the Program screen, click the Upgrade button.
5. Click Finish on the Completing the Microsoft Operations Manager 2005 Setup Wizard screen to complete the upgrade.

Upgrading MOM Agents

If a manual upgrade is required for many agents, they can be deployed using software deployment mechanisms such as Group Policy or Systems Management Server (SMS).

Uninstall MOM 2000 Reporting

If your MOM 2000 environment had the reporting components installed you can now manually remove these from your environment if they are not being used by other applications. To uninstall the reporting components:

1. Log in to the reporting server.
2. Launch the Add or Remove Programs Wizard.
3. Remove the Microsoft Access 2000 Runtime or Full Version.
4. Remove the Microsoft Office Graphic Components.

Maintaining Report Information

Uninstalling MOM 2000 Reporting removes all reporting information from the Microsoft Access database. To retain this data either extract it or do not delete the database.

Import Management Packs

When you upgrade your MOM environment, the final step in the upgrade process is importing management packs. Prior to importing management packs you should review what servers you will be monitoring, what their functions are, and what management packs are required for your particular environment.

Real World—Installing Management Packs

Resist the urge to install everything and see what happens. Trust us, it is not pretty. For those of you who don't trust us, we will go into more detail:

- If you install all management packs you will receive information from all MOM agents that have the relevant criteria (for example, if you install the IIS management pack, MOM will monitor IIS on all managed systems with IIS). The resulting flood of information makes it difficult to determine what is really an issue versus what is not important for your particular environment.
- The amount of data being returned per server increases significantly and increases the size of the OnePoint database.
- There is no process that completely uninstalls a management pack after it has been installed. Although there are procedures to remove management packs they do not completely remove all components.
- As more rules are pushed to an agent it results in more CPU, memory, and disk requirements for the MOM agent.

- The additional information results in increased utilization of the MOM servers and can lead to overloaded queues or even cause MOM to stop functioning properly.

We recommend that you install only the management packs that are most important first and then phase in additional management packs over time rather than deploying everything at once.

As discussed in Chapter 4, we recommend establishing a proof of concept environment. This environment can be retained for testing patches and upgrades to your MOM environment.

Details on management packs and their installation processes are available in Chapter 13, "Administering Management Packs." Review Chapters 15, 16, 17, and 18 for further information regarding use of specific management packs.

Troubleshooting Tips

Table 7.2 details some potential errors that may occur when upgrading MOM 2000 SP1 to MOM 2005. The Knowledge Base Article Number can be used to get more detailed information in the Microsoft knowledge database at http://support.microsoft.com.

TABLE 7.2 Common Errors When Upgrading

Process Erroring	Error Message	Potential Cause	Knowledge Base Article Number
2005 Upgrade	"Prerequisite Check Did Not Pass" message.	This problem may occur if you previously installed the Microsoft SQL Server 2000 update SQL2000-KB810185-8.00.0859.	885462
2005 Upgrade	All the queries in a query expression containing a UNION operator must have the same number of expressions in their select lists.	Changes to the schema of the database through either SQL Server Replication or manual alteration of the OnePoint database.	885722
2005 Upgrade	Failed to create MOM Database. Error Code -2147221164 (Class not registered).	Issue with the Oledb32.dll file, which can result on computers upgraded from Windows 2000.	885734
2005 Upgrade	In the MachineNameAgentInstall.log file or in the MOMComponent.log file; "ForceKillMOMHost: Setup failed to kill MOMHost process. Error Code: 0x80070424."	This likely indicates that the MOM service has been deleted from the previous MOM installation.	888833

TABLE 7.2 Continued

Process Erroring	Error Message	Potential Cause	Knowledge Base Article Number
2005 Agent Upgrade	On the Details on the Microsoft Operations Manager Task Progress dialog box: "Failed DOMAIN\ServerName. The agent management task timed out while processing the requested operation for managed computer ServerName. FQDN.com…"	This likely indicates that the workstation was previously upgraded from MOM 2000 to MOM 2000 SP1.	887309
After 2005 Upgrade	Event ID: 9122 appears in the Application log and agents cannot communicate with the management server after you install MOM 2005 or upgrade to MOM 2005.	This problem occurs if you use a NetBIOS domain name that contains a period.	889187

Upgrading MOM 2005 Workgroup Edition

Along with the full edition of MOM 2005, Microsoft has created MOM 2005 Workgroup Edition. Workgroup Edition is designed for small-sized businesses that require management of fewer than 10 devices. Microsoft Operations Manager 2005 Workgroup Edition is a cost-effective solution because it requires only one license for the server itself and no licenses for the devices being managed by MOM. The workgroup edition provides a subset of the MOM 2005 functionality with restrictions that are described in Chapter 2, "What's New."

The process to upgrade from MOM 2005 Workgroup Edition is relatively straightforward because all MOM components are installed on a single server. Often a migration from MOM 2005 Workgroup Edition to MOM 2005 is precipitated by business requirements that can no longer be met with the Workgroup Edition but instead will require the full version of MOM 2005. These requirements should have been identified during the assessment phase (see Chapter 4).

Common requirements include increased scalability, integration with other MOM servers, and reporting capabilities. The following questions should be answered before starting the upgrade process:

- Will the full MOM 2005 environment still have the database server on the same server?—Adding an external database server can increase the scalability of your MOM environment, and if it is installed on a clustered SQL solution this can also increase the redundancy of your MOM configuration.

- Do you plan on installing the Microsoft Operations Manager Connector Framework (MCF)?—The MCF functionality is not available in MOM 2005 Workgroup Edition. MCF is a web service-based technology that allows MOM to connect with other third-party management platforms. If you need to connect MOM to another management platform consider installing MCF. The MCF is discussed in Chapter 19, "Interoperability."
- Do you plan on installing the MOM Reporting Components?—Reporting is also not available in MOM 2005 Workgroup Edition. If reporting is a requirement for your MOM environment you need to consider an upgrade and then what server to use to provide this function.

Database Changes When Upgrading from MOM 2005 Workgroup Edition

If your MOM 2005 Workgroup Edition installation uses MSDE rather than SQL Server, you need to first upgrade the MSDE to SQL Server 2000 before beginning the MOM 2005 upgrade process.

Upgrade Overview

When upgrading from MOM 2005 Workgroup Edition to MOM 2005 full edition, it is important to prepare for the upgrade and to create and verify a successful backup of your management server. After a successful backup, the process involves running the full edition setup for MOM 2005; afterwards additional components such as MOM Reporting can be installed.

For this example, MOM Workgroup Edition is installed on a system named Littleton, which is running all Workgroup Edition components on a single server and has agents on Loveland (the domain controller) and Cortez (the terminal server). Figure 7.7 shows the Littleton server and the agents installed on Loveland and Cortez.

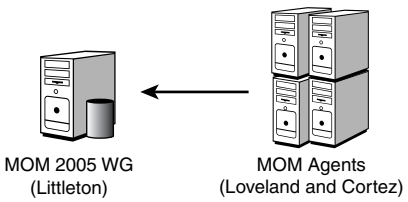


FIGURE 7.7 A single server named Littleton running MOM 2005 Workgroup Edition.

MOM 2005 Workgroup Upgrade Detailed Steps

When upgrading from MOM 2005 Workgroup edition to MOM 2005, the following steps are required.

1. Back up the MOM 2005 Workgroup Edition server. If the server is either not being backed up currently or the backup process has not been tested, review Chapter 12, "Backup and Recovery," which discusses the MOM 2005 backup process.
2. Run the Microsoft Operations Manager 2005 Setup Resources program, setup.exe.
3. Check prerequisites for the MOM database, management server, and MOM user interface. If applicable, also check the prerequisites for the MOM Connector Framework, MOM product connectors, and the MOM 2005 web interface. (At this point we do not need to resolve MOM 2005 Reporting prerequisites; we can address them after upgrading to MOM 2005.)
4. After resolving any prerequisite issues, on the main menu of the MOM setup choose the Install Microsoft Operations Manager 2005 option.
5. If MOM 2005 Workgroup Edition is detected, the Upgrade Microsoft Operations Manager screen previously shown in Figure 7.5 is displayed. Click on the Upgrade to MOM 2005 check box.
6. The first few screens of the wizard are fairly typical. You will accept the license agreement and enter user information and your product key.
7. The setup process automatically runs the prerequisite check prior to starting the upgrade. Resolve any errors on the prerequisite checking page and note any warnings to either resolve prior to or after the upgrade process.
8. Enter your Management Server Action account username, password, and domain. If this account is not a domain administrator, it should be added into the local Administrators group on the server prior to continuing.
9. Now enter your Data Access Server account username, password, and domain.
10. At the MOM Error Reporting screen check the Enable Error Reporting option and take the default of Automatically Send Reports to Microsoft.
11. Next, click the Install button on the ready to install screen. MOM 2005 has begun the process of upgrading!
12. Accept the default to Start the MOM Administrator console. Click on the Finish button after the process has completed.
13. Validate that the Administrator console now shows that the full version of MOM 2005 is installed. This can be verified by opening the Administrator console, right-clicking on the Microsoft Operations Manager (servername), and checking that the screen no longer says Congratulations on your installation of Microsoft Operations Manager Workgroup Edition but rather says Congratulations on your installation of Microsoft Operations Manager. Also verify that MOM agents are still reporting their status correctly within the MOM Operator console.

14. If installation of the MOM Reporting components is a requirement, refer to Chapter 6 for details related to the MOM Reporting prerequisites and installation process.
15. Import any additional management packs.
16. Deploy agents to additional servers at this time.

Summary

In this chapter we investigated the process for upgrading the MOM 2000 SP1 environment ranging from the simplest to complex configurations and detailed the steps required to upgrade from MOM 2005 Workgroup Edition to the full version of MOM 2005. The next chapter provides information on post-installation tasks.

This page intentionally left blank

PART III
Deploying MOM

IN THIS PART

This page intentionally left blank

CHAPTER 8

Post-Installation Tasks

IN THIS CHAPTER

This chapter discusses tasks to be performed after installing Microsoft Operations Manager (MOM). We assume MOM 2005 is installed. If that is not the case, you may want to first read Chapter 6, "Installing MOM 2005," to step through a fresh install, or Chapter 7, "Upgrading to MOM 2005," if you will be upgrading from a different version of MOM (either MOM 2000 or MOM 2005 Workgroup Edition).

If you are familiar with a different version of MOM, you most likely will approach this chapter to become acclimated to this release of Microsoft's server monitoring software and its user interfaces. In this case we suggest you read through Chapter 2, "What's New," as an introduction. Chapter 2 describes the differences between MOM 2005 and MOM 2000 as well as with MOM 2005 Workgroup Edition. If you are entirely new to MOM, focus instead on this chapter to familiarize yourself with MOM 2005.

This chapter discusses basic configuration and administration of MOM 2005. You will learn about the functions and components of the MOM consoles, and how to install them on remote machines. We step through wizards in the Administrator console to install agents and management packs. We also discuss MOM security groups and how they are utilized with the Administrator and Operator consoles, database maintenance for the MOM database, and administering MOM 2005 Reporting.

Processing Flow of the MOM Environment

First, a quick review of the MOM components: The basic management unit in a MOM 2005 environment is the management group, which includes a MOM database, one or more MOM management servers, and MOM agents. Data

flows between the MOM database, the management server, and managed computers. This flow is bidirectional, with the direction determined by the particular situation. Data can include operational data, rules, and configuration information. Figure 8.1 illustrates the data flow; additional details on processing flow can be found in Appendix A, "Mom Internals."

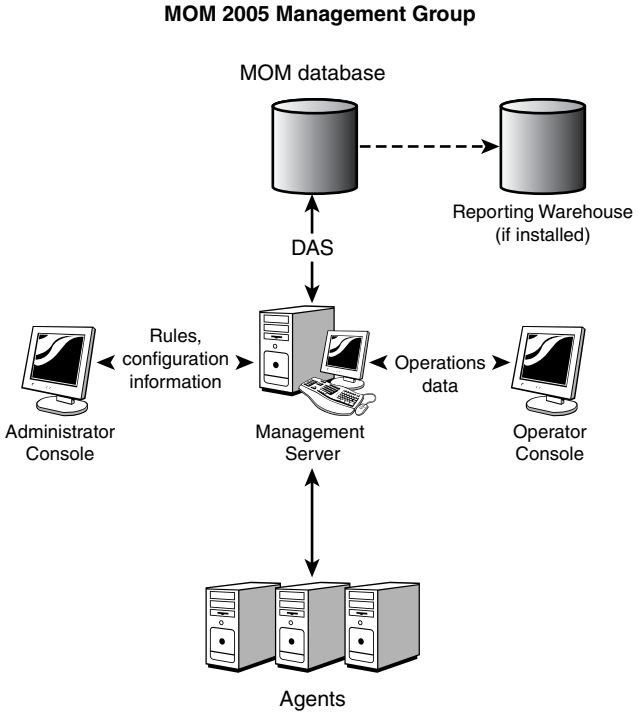


FIGURE 8.1 Management group data flow.

Operational Data

Agents on managed computers monitor activities and collect operational data. The information is sent to the management server in the form of alerts, events, and performance counters. Often such information indicates some form of degraded performance. The MOM Server component passes the data to the Data Access Service (DAS) component, which adds the information to the MOM database. The information is then sent to the Operator console.

If the computer is configured for agentless monitoring, the local agent on the management server raises the alert and passes the data to the DAS. Additional information on agents is provided in Chapter 9, "Installing and Configuring Agents."

Rules and Configuration Information

Management packs for specific applications and services contain the rules used by MOM. Configuration information for MOM is loaded during installation.

Rule changes to management packs and configuration changes to settings are made using the Administrator console. The MOM Server component passes that information to the DAS, which writes the change to the MOM database. After the change is committed to the database, the management server sends these changes to its managed computers. Changes for agentless managed computers are implemented by the local agent on the management server.

Data Collection

The agent sends operational data collected during monitoring to the management server, where it is stored by the DAS component in the MOM database. This data includes event, performance, alert, and discovery information.

Information captured by the agent is presented as operational data, graphs, reports, state views, topology diagrams, service lists, and computer lists. The information is available in the Operator console, the Web console, or the Reporting console.

MOM 2005 Consoles Overview

The MOM 2005 consoles include the Administrator, Operator, Web, and Reporting consoles:

- **Administrator console**—This console is where you configure MOM 2005, discover systems, deploy agents, create and maintain user privileges and console scopes, and create, maintain, import, or export management packs.

  The Administrator console is a Microsoft Management Console (MMC) snap-in that provides management pack administration and MOM server-level configuration, and is where you configure and manage MOM itself. As an MMC application, the console is divided into two panes. The left-hand pane is the Navigation Pane, which contains the console tree with nodes; the right-hand pane is the Detail Pane, which displays the specifics of a particular node selected in the Navigation Pane. Figure 8.2 illustrates the Administrator console.

- **Operator console**—The MOM 2005 Operator console provides a view into the health of your systems, indicates problems that have occurred, and recommends resolutions. This console is used to manage alerts and monitor the operational status of your systems.

  The Operator console utilizes multipaned views, which allow you to easily see the information necessary to resolve a problem without having to open multiple windows or dialog boxes. The console includes the following capabilities:

  - **State view**—Sometimes referred to as "at a glance" status, the Operator console is based on the Microsoft Outlook 2003 interface and provides access to a group of monitored servers. Central to the visuals on this console is its roll-up status displays. Server status is represented by green, yellow, and red icons.

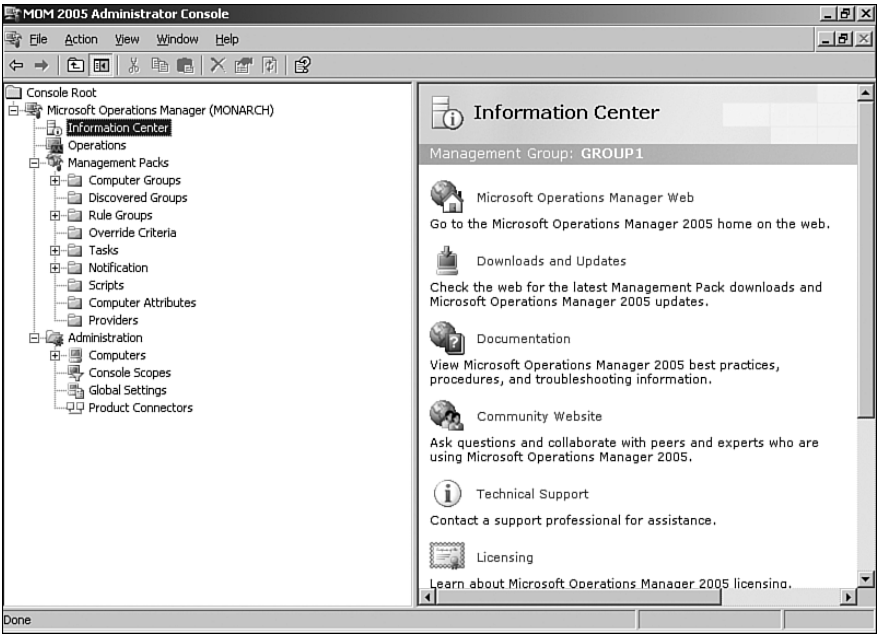


FIGURE 8.2 The MOM 2005 Administrator console.

When a server shows a yellow icon, that server's capabilities are impaired; a red icon indicates a severe problem. By quickly glancing at the column headers, you can get an instant view of the condition of the services running on your network with the ability to double-click on a server and quickly drill down to a particular problem area.

- **Perform tasks**—The Operator console includes the capability to launch operations-related tasks, such as starting and stopping services or checking network statistics. These tasks are generally defined in management packs, or you can create and maintain them yourself using the Administrator console.
- **Diagram view**—This gives you a visual representation of network topologies as defined by various management packs. It graphically displays managed servers and uses status icons to indicate any problems. You can even export diagrams to Visio, giving you a quick and easy way to create accurate network drawings for later use.

Figure 8.3 displays the Operator console with the "at a glance" roll-up with one server having a red icon, and one system with a green icon. The Alerts Pane gives information regarding the server with a critical (red) error.

- **Web Console**—The Web console provides a subset of the Operator console functionality using a web browser. It incorporates the Alerts, Computers, and Events views of the Operator console, and gives you the flexibility from anywhere on the network to easily modify the status of an alert, view company knowledge, check the status of a computer, or look at a specific problem that needs attention.

The Web console is accessed using the format http://*server:port,* where *server* is the NetBIOS name of the management server, and the Transmission Control Protocol (TCP) *port* by default is 1272. The console uses Windows Integrated authentication and is intended for intranet use only. Figure 8.4 shows the Web console.

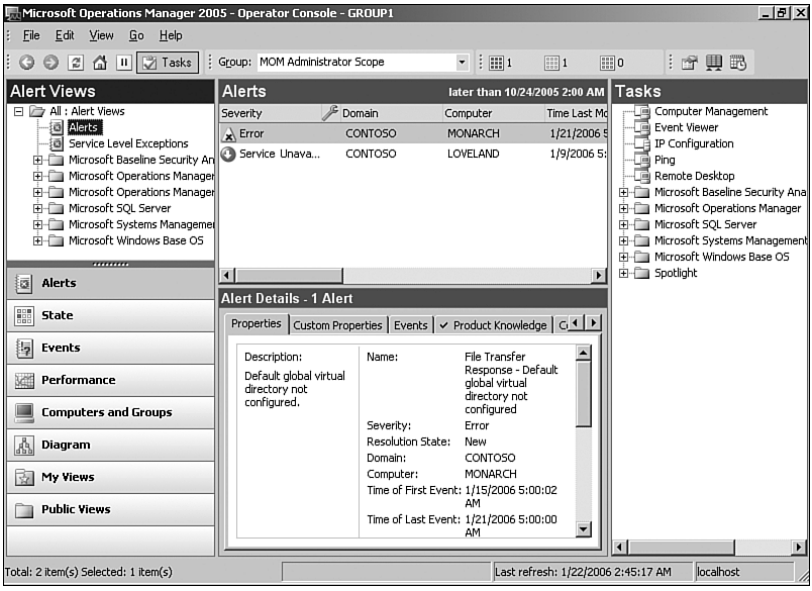


FIGURE 8.3 The MOM 2005 Operator console.

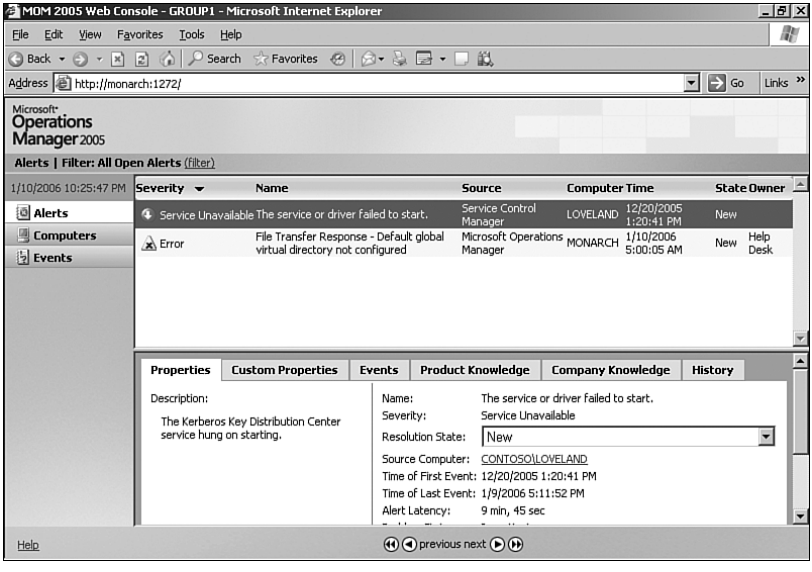


FIGURE 8.4 The MOM 2005 Web console.

- **Reporting Console**—The Reporting console allows you to view event, alert, and performance reports using a web browser interface. You can subscribe to favorite reports and automatically receive new versions as those reports are updated with new information.

  MOM 2005 uses Microsoft SQL Server Reporting Services for its reporting engine, giving you the built-in capabilities of that software. You can authorize individuals to have operational status reports regularly delivered via email, or generate a PDF or web-based report to an intranet web page on a scheduled basis. Figure 8.5 illustrates a sample Reporting console.

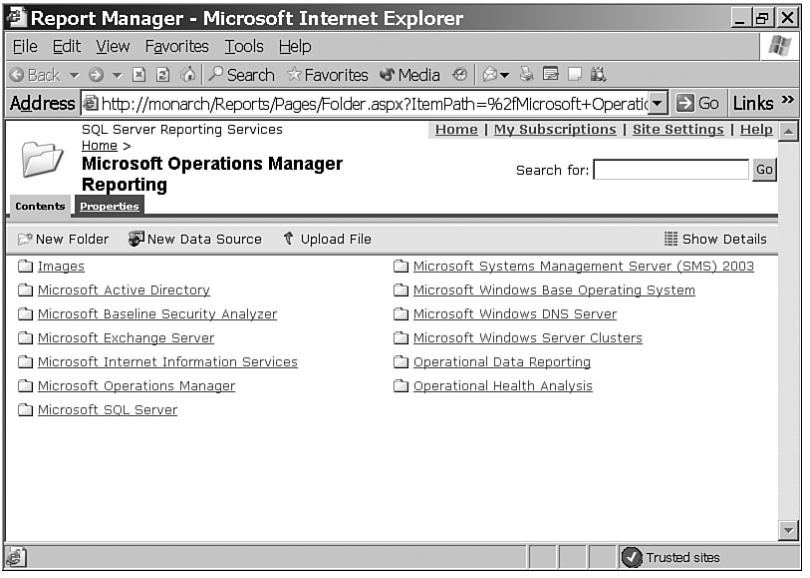


FIGURE 8.5 The MOM 2005 Reporting console.

Before taking a closer look at the Administrator and Operator consoles, let's talk about MOM security groups. Although security groups are covered extensively in Chapter 11, "Securing MOM," an overview at this point provides information for understanding how MOM security groups influence your usage of these two consoles.

When you install MOM 2005 into your environment, it creates a number of local security groups that are used to manage access to MOM features. Three of these groups pertain to usage of the Administrator and Operator consoles:

- **MOM Administrators**—These have full access to all features in MOM and to the MOM consoles. MOM Administrators can view and change settings in the Administrator console and the Operator console, as well as in all the nodes of these consoles.
- **MOM Authors**—Authors have full access to the Operator console where they can view and change settings for the Operations and Management Packs nodes but

limited access to the nodes in the Administrator console. MOM Authors cannot maintain Agents.

- **MOM Users**—These can view and modify settings in the Operator console and have access to the Operations node of the Administrator console only.

What you can do in any particular console—in fact how much you will see—depends on the security privileges your user account has. These privileges are based on its MOM security group membership. As an administrator, you can use these three groups to define and structure console access for individuals in your organization.

We will now take a detailed look at the Administrator and Operator consoles.

Drilldown: MOM 2005 Administrator Console

The MOM Administrator console is used to configure and administer MOM. Remember you must be logged on as a member of the MOM Administrators group to view all the nodes in the console Navigation Pane and have access to all administration tasks.

Getting Started with MOM

When you first open the MMC snap-in for the Administrator console after installing MOM, the Detail Pane (shown in Figure 8.6) displays three setup tasks, known as Quick Start Options, for completing your MOM installation:

The Three Setup Tasks

The three tasks displayed in Figure 8.6 are available to MOM Administrators only.

- **Install Agents**—MOM needs to know which computers to monitor before it starts monitoring them. Selecting Install Agents launches the Install/Uninstall Agents Wizard, which you can use to specify computers or give discovery parameters to add computers to your management group.
- **Import Management Packs**—After MOM knows what computers to monitor, it needs to know what information you want to monitor. Management packs define services and components to be monitored. The only management pack automatically installed with MOM is the one monitoring MOM 2005 itself.
- **Start Operator Console**—After you have defined computers to monitor and services to be monitored, you can start the Operator console to view the status of the computers being monitored.

Managing agents and utilizing management packs are covered at length in subsequent chapters, but we will discuss some basic configuration now so that you can become familiar with configuring and administering MOM 2005.

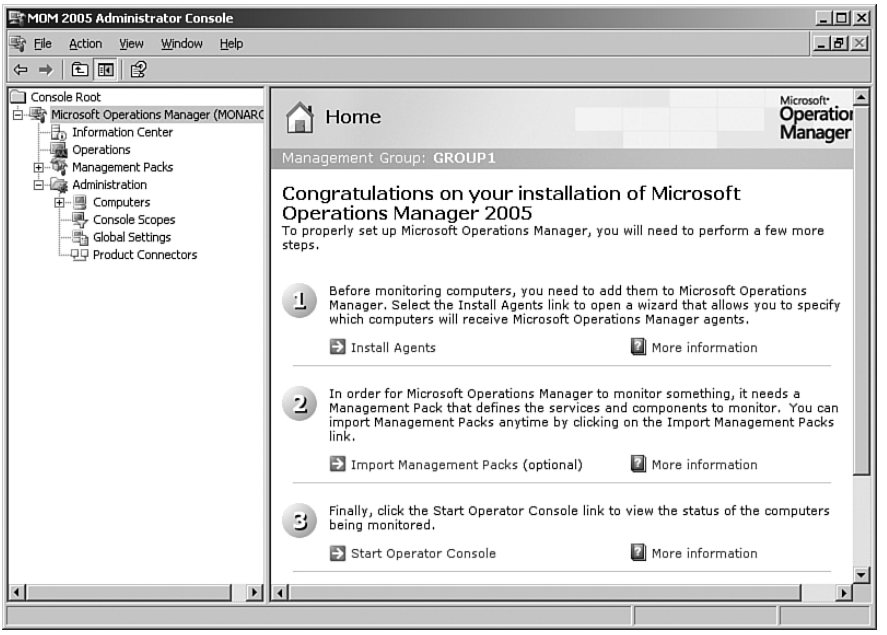


FIGURE 8.6 The Home view of the Administrator console.

Quick Start—Install Agents

To install an agent, click on the Install Agents selection in the detail Quick Start Pane, which you can access by selecting the top level of the Administrator console. The Install/Uninstall Agents Wizard walks you through the process of installing an agent. Behind the scenes, the wizard creates a discovery rule to locate one or more computers using the criteria you specify. The following steps install an agent on the Loveland server:

1. You are asked to browse for or type in a specific computer name, or to enter search criteria. Because we are doing just the "bare bones" here, select the Browse option and click on Next.
2. On the Computer Names screen of the wizard, type in the name of a computer, in this case our domain controller Loveland; then proceed to the next two screens to select the defaults of using the Management Server Action account to install the agent and specifying the Local System account as the Agent Action account.
3. You are then asked to indicate the directory to install the agent into; again, take the default.

The wizard now has all the information it needs, and it proceeds to schedule the task, install the MOM agent on Loveland, and notify you when the installation is complete. The agent installation adds the MOM service and the %*ProgramFiles*%/Microsoft Operations Manager 2005 folder to the managed computer.

Quick Start—Import Management Packs

As previously mentioned, the only management pack loaded with the MOM 2005 install is the Operations Manager (MOM) 2005 Management Pack, which lets you see such things as whether the agents (when installed) are missing heartbeats, or whether the SQL Server maintenance jobs against the MOM OnePoint database are running. At this time we will import the Windows Server Base OS Management Pack into our management group so that you can begin to understand how management packs work. Management packs and their components are discussed in more detail beginning in Chapter 13, "Administering Management Packs."

Getting Current Versions of Management Packs

Some of the MOM 2005 management packs can be found on the MOM 2005 installation CD, but to ensure that you are getting the most current version of any management pack it is best get them online.

Management packs can be found online at the Microsoft Management Pack catalog at http://go.microsoft.com/fwlink/?linkid=43970. By selecting Operations Manager 2005 as the MOM Version for the query and specifying Microsoft Operating System Components as the Management Pack Category, you will see the various management packs available related to operating system components. Figure 8.7 shows the selection criteria available to search for management products.

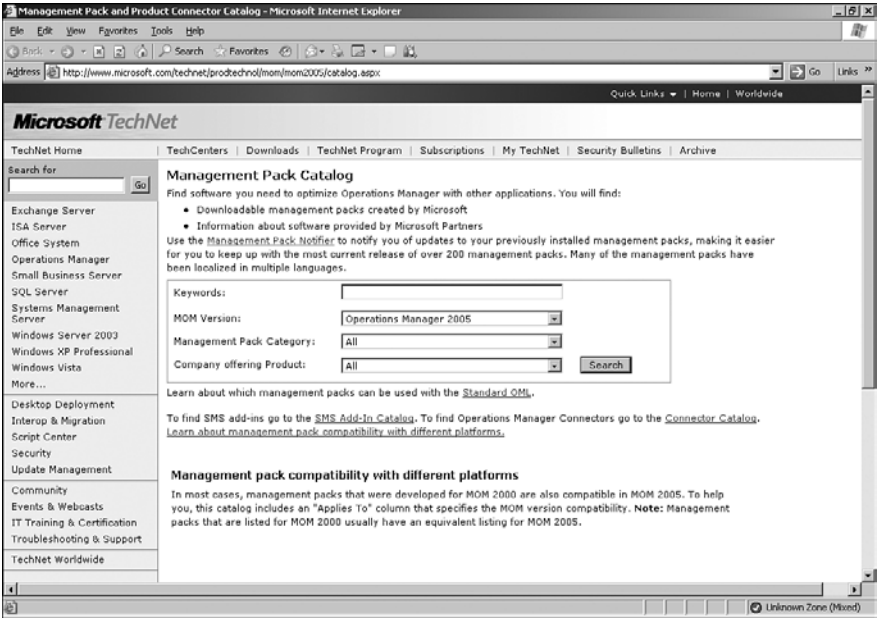


FIGURE 8.7 Selection criteria using the Microsoft Management Pack Catalog.

Third-Party Management Packs

A number of third-party management packs are available for MOM 2005 and listed in the Management Pack Catalog. We describe some of the more significant third-party management packs in Chapter 19, "Interoperability," and in Chapters 15 through 18 as extensions for monitoring particular applications. Your particular environment will dictate which are most appropriate for your use.

To search for a particular management pack by name, you would select All as a Management Pack Category and type in a phrase such as "Windows Server Base OS" in the Keywords box. The returned results display only the most recent version of any particular management pack. Be sure to specify the MOM Version of Operations Manager 2005 as part of your query.

Locate the Windows Server Base OS (Server) 2000, 2003 Management Pack in the Product List. Selecting it takes you to the download section of Microsoft's website. Download the file and then execute it. The extraction process places the contents of the software package into a folder named \Microsoft Windows Servers Base Operating System MOM 2005 Management Pack. The folder contains the following files:

- MOM 2005 Supplemental End User License Agreement (English).rtf—An end-user license agreement
- MicrosoftWindowsBaseOperatingSystem.akm—The source file for the management pack itself
- MicrosoftWindowsBaseOperatingSystemReports.XML—The report definitions used when MOM Reporting is installed
- Base OS MP Guide.DOC—The management pack guide for this particular management pack, which includes documentation regarding the management pack

You can expect a similar file structure with other management packs authored by Microsoft, although the contents may differ. A management pack guide may or may not be included with the downloaded package, and the XML file is present if reports are defined for that particular service or application.

Finding Management Pack Guides

The MOM 2005 Management Pack Guides can also be located on Microsoft's website at www.microsoft.com/technet/prodtechnol/mom/mom2005/maintain.

You now have extracted the management pack source file (.akm) you need to your local file system. You still must load the management pack itself into MOM 2005. This is accomplished using the Management Pack Import/Export Wizard in the Quick Start Pane.

Invoking the Import/Export Wizard

You may also invoke the Import/Export Wizard by right-clicking on management packs in the Navigation Pane of the Administrator console and selecting Import/Export Management Pack.

Starting the Import Wizard walks you through the steps to import the management pack into your MOM installation:

1. On the Import or Export Management Packs panel of the wizard, choose Import Management Packs and/or reports. Browse to the folder where you extracted the contents of the downloaded Microsoft Windows Servers Base Operating System MOM 2005 Management Pack.

   If you have not installed MOM Reporting, the wizard gives you the option to import management packs only.

2. Select the management pack to be imported, select whether you want to update the existing management pack or replace it, and select whether you want to back up the management pack. It is not necessary to back up the previous version if the management pack was not already imported into MOM. Figure 8.8 shows available import option choices.

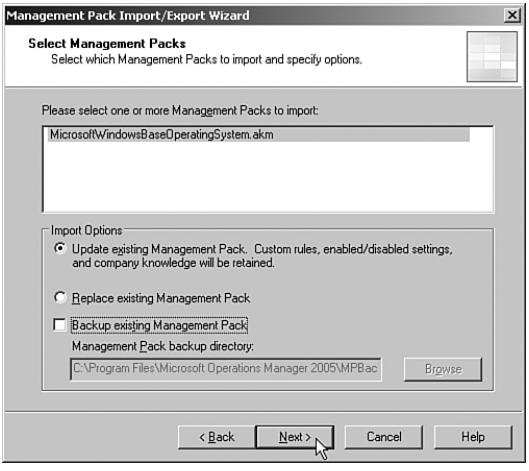


FIGURE 8.8 Specify import options in the management pack Import/Export Wizard.

3. After specifying the criteria for importing the management pack, the wizard loads the management pack into MOM, providing a status report of its actions. You may save the report in a log file if you want.

The Quick Start Pane now suggests that you start the Operator console, but prior to that let's continue to look at the MOM Administrator console. The Administrator console has two major areas of administration: Management Packs and Administration of the MOM infrastructure itself.

Maintaining Management Packs

The Management Packs section of the Administrator console is used for importing and exporting management packs, changing the contents of a particular management pack, and creating new components for a management pack. Selecting Management Packs on the left pane of the MMC console brings up a summary of the management pack information known to this particular management group, as shown in Figure 8.9.

Limitation of MOM Users

Management packs cannot be maintained by the MOM Users security group. You must be a member of the MOM Administrators or the MOM Authors local security group to maintain management packs.

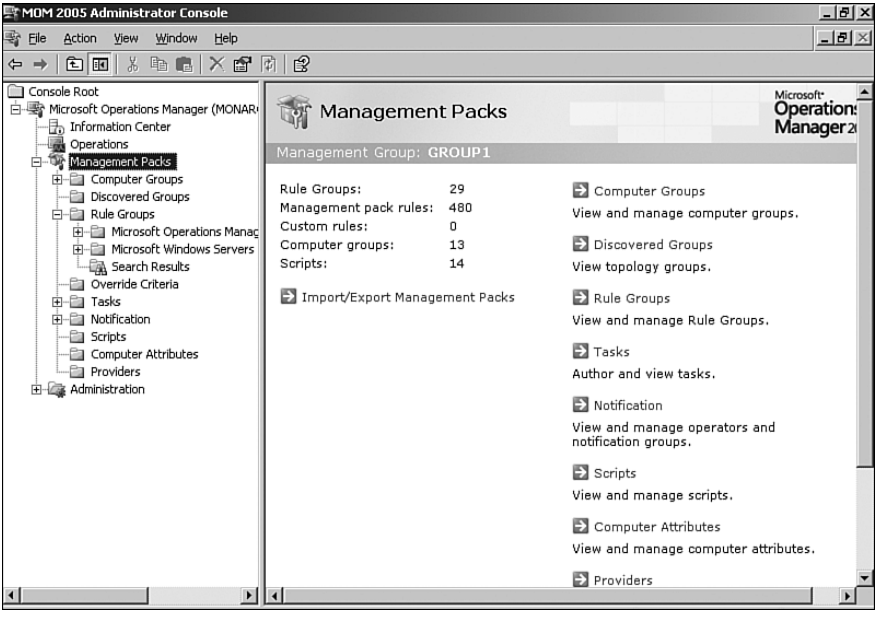


FIGURE 8.9 The Management Packs folder in the Administrator console.

Rule Groups

Looking now at the Navigation Pane, notice that we have rule groups for Microsoft Operations Manager and Microsoft Windows Servers Base Operating Systems; yet the right-hand (Detail) pane indicates some 29 rule groups. Why is there this apparent discrepancy? Rule groups can be nested; if you were to drill down through the two rule

groups on the left-hand panel you would discover there actually are a total of 29 rule groups detailed, with 480 management pack rules between them.

The Detail Pane also notifies us that there are no custom rules (company-specific rules your organization has created), and that in addition to rule groups there are 13 computer groups and 14 scripts. All of these objects were loaded in with the management packs.

Objects in a Management Pack

The count of objects within a management pack may change as Microsoft or any third-party vendor releases new versions of a management pack. These particular numbers refer to versions of the Windows Server Base Operating System Management Pack and the Operations Manager (MOM) 2005 Management Pack available when this book was written in 2006. Newer versions of these management packs may have a different number of objects.

Let's look briefly at the other components listed in the Management Packs folder. Management packs are discussed in greater detail in Chapter 13.

Computer Groups

Computer grouping rules are used to classify systems with particular attributes as belonging to a computer group. In our case we have computer groups defined with the Microsoft Operations Manager or the Windows Server Base Operating System management packs.

Discovered Groups

The Discovered Groups folder contains any computer groups discovered by MOM. You can create a replica of a discovered group by right-clicking on a discovered computer group. Replica groups are regular computer groups based on the membership of a discovered group. You would use a replica group when you want to use a discovered computer group for one (or more) rule groups. A discovered group cannot directly be associated with a rule group.

Override Criteria

This folder is a convenient way to view all unassociated override criteria in the management group. Unassociated override criteria are not attached to any rules and can be used to share overrides among different rules. Developers can also reference these overrides in scripts.

Using the Override Criteria Folder

Without this folder unassociated overrides would be difficult to track. The default names for overrides also point out the importance of practicing naming standards because the default names are not intuitive (for example: {2AD7F6A7-DD6A-4F95-9BC2-BE58188E00FC}.

In a large management group there can be many overrides, and this folder gives you the ability to identify those that are not associated with any rules.

Tasks

Tasks are actions that diagnose or repair a problem, or that automate a management process. Tasks are defined in the Administrator console and executed in the Operator console. Tasks can apply to alerts, events, or computers. Although tasks are typically implemented as part of a management pack, an administrator can create specific tasks as needed.

Notification

One possible response to an event or an alert is to notify an individual through an automated mechanism such as email or a pager. Most predefined alerts are configured to send a notification message.

Notification Groups Notifications are sent to members added to notification groups. The notification groups are typically created by management packs. For example, the Microsoft Operations Manager Management Pack uses two notification groups: Operations Manager Administrators and Operations Manager Notification Testing. The Windows Base Operating System management pack includes the Network Administrators notification group.

You can create your own notification groups as well. For example, you might want to create a notification group for your help desk.

Operators Notification groups contain operators, which you must define for your organization. *Operators* are objects used to store information about people to notify when there is a particular alert or condition. An operator can belong to multiple groups. Each operator entry includes the capability to specify several notification methods including an email address, a pager number, or an external command. You can also specify days and time blocks to notify an operator, so that some people can be notified during work hours, and others on nights or weekends.

Configuring Email Notifications

Knowledge base article 920736 (http://support.microsoft.com/kb/920736/) provides configuration steps for email notifications in MOM 2005.

Paging is enabled by sending an email to a paging service. The paging service must support Simple Mail Transfer Preotocol (SMTP) email for MOM paging to work. External commands may be used to page operators through a modem rather than using the SMTP email service. The command itself is specified within the rule that fires the response to the notification group.

Using Email to Notify About Email Status

One often-cited dilemma of using an SMTP email service for notifications is if the notification concerns Exchange the warning may not be delivered—because the mail server is not available! However, with an external command-line tool, you can use third-party messaging applications to notify operators of detected conditions.

Scripts

A script consists of instructions added to a rule as a response or used to extend event criteria definition. Scripts can run on an agent-managed computer or the management server. This folder can be used to mange scripts running on agent machines.

Computer Attributes

Computer attributes are used in formulas to populate computer groups with member computers. Computer attributes will either be based on registry keys or registry values for a specific computer, or based on service discovery.

Providers

This folder lists the current data providers. Providers are listed by type, name, and settings that describe what the provider offers. Examples of providers include performance counters, the event logs, and timed events. Use of providers in rules is discussed further in Chapter 14, "Monitoring with MOM."

MOM Administration

The Administration node of the console is used to configure various settings for a specific management group. These include maintaining computers and agents; setting console scopes; maintaining global settings; and if the MOM Connector Framework is installed, maintaining product connectors, which are used in configuring multitiered MOM environments. Product connectors are discussed in Chapter 19. Administrators should also be aware of the scheduled maintenance jobs that run in a management group.

Computers

The Computers section allows you to view all computers in a management group, install and maintain agents, specify how an individual computer is managed, and maintain properties for individual computers. Agents are discussed in Chapter 9.

Console Scopes

A console scope consists of a set of computer groups and a list of users who can access those computer groups. Because users can be associated with only one console scope at a time, they can be granted access to only one set of computer groups.

The Console Scope Utility

Out-of-the box, MOM 2005 requires you to manually maintain the users in console groups. However, you can use the MOM 2005 Resource Kit Console Scope Utility, CSUtil.exe, to synchronize the MOM console scope members with members of Active Directory Groups. CSUtil is run on a management server. The following parameters can be used with CSUtil.exe:

```
CSUtil.exe Action ScopeName TargetName
<Action> The action to perform. Valid action types include:
- CreateScope: Creates specified console scope.
- DeleteScope: Deletes specified console scope.
- AddUser: Adds a user to console scope.
```

```
- RemoveUser: Removes a user from console scope.
- Synchronize: Synchronizes console scope members with those in the named
Active Directory group. If the scope does not exist, it is created. If the
Active Directory group does not exist, the console group is deleted.

<ScopeName> [TargetName] The MOM scope name to use. If the scope does not
exist, it is created. If you specify an empty string rather than a TargetName,
the scope name is assumed to be the same as the Active Directory group name.
```

The Console Scope utility requires MOM 2005 SP1.

Console scope settings define the computer groups that individual MOM 2005 users see in the Operator console and applications built using the MOM Software Development Kit (SDK). A console scope acts as a filter, which makes it easier for users to monitor the computer groups and computers they are responsible for.

Three console scopes are created by MOM 2005: the MOM Administrator Scope, the MOM Author Scope, and the MOM User Scope. You cannot add users directly to the built-in scopes; these scopes utilize local security groups, which are maintained using the Computer Management MMC snap-in. Using the Administrator console, you can create your own scopes as necessary to control the access and functionality individuals have to the consoles and add users to those scopes.

Use Custom Scopes for Security

We suggest using custom scopes as a tool to compartmentalize your operations environment.

Global Settings

MOM Administrators have the capability of changing a number of global settings. These include a variety of settings such as adding alert resolution states, changing service level agreement specifications, configuring email server settings, changing the TCP/IP port used by MOM and its agents, specifying a new address for the Web console, changing the time and frequency for running computer and attribute discovery, and modifying the installed database grooming settings.

The management server scans the network for all managed computers every 24 hours to detect any changes or modifications. The scan process, which occurs by default at 2:05 a.m., accesses Active Directory for the names of computers belonging to the domain, reads registry keys or values on those systems based on particular computer attributes, and identifies the components used by that computer.

Scheduled MOM Database Maintenance Tasks

To maintain the performance and health of the MOM database, a number of database maintenance tasks are created during your MOM installation. These tasks are defined as

SQL Server jobs, and you can use the SQL Server administration tool to monitor the status or change the scheduled runtime for any database job—under Management \ SQL Server Agent \ Jobs.

Although most of these tasks perform typical types of database maintenance, several are specific to aging and archiving the operational data stored in the OnePoint database. These two jobs—*OnePoint – Update Database* and *MOMx Partitioning and Grooming*—are parameter driven, using grooming settings defined in the MOM Administrator console under Administration \ Global Settings \ Database Grooming. Figure 8.10 shows the default settings. A third job of interest is the *OnePoint – Reindex* job. These three jobs include the following functionality:

- The Update job runs hourly, by default on the half hour, and sets alert status to Resolved after an alert ages past the time limits defined by the Grooming settings. These settings specify when outstanding alerts will be automatically resolved and can be specified in terms of days, hours, or minutes.
- The MOMx Partitioning and Grooming job runs nightly at midnight. It grooms resolved alerts from OnePoint.
- The Reindex job runs every Sunday at 3:00 a.m. by default. This job rebuilds indexes used by the OnePoint database and requires 40% free space in the database. The Reindex job fails if you do not have enough free space. MOM continues to function if the indexes are not updated, but database response time eventually increases as the indexes become more out of date.

Avoiding Slow Report Generation

It is also important to perform maintenance on the data warehouse, because a lack of maintenance results in slow report rendering. The crew at momresources.org has published a script to assist with optimizing the index performance, available at http://www.momresources.org/momscripts/scdw_reindex.zip.

The MOM Databases Are Not Automatically Backed Up

You should create tasks to back up the SQL Server databases that MOM uses. Many organizations, including a number of Fortune 500 companies not using SQL Server as their enterprise database engine, do not realize backup jobs are not created during the MOM setup process. Chapter 12, “Backup and Recovery,” discusses the steps and procedures to establish SQL Server backups for your MOM databases.

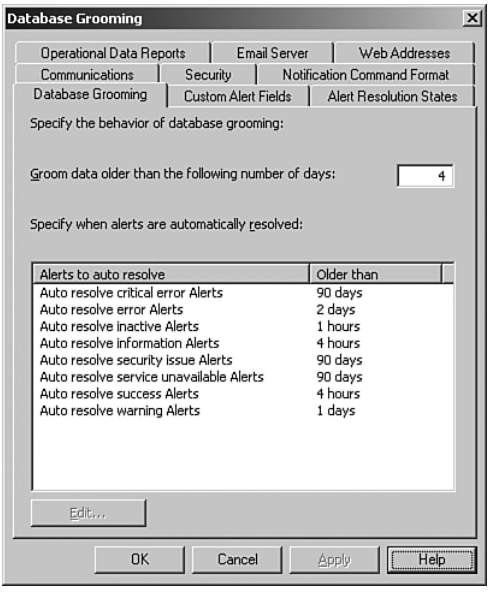


FIGURE 8.10 The database grooming settings.

Drilldown: MOM 2005 Operator Console

The MOM Operator console can be accessed as a link through the MOM Administrator console or directly through the Microsoft Operations Manager 2005 program group in the Start menu. The console is used to monitor events occurring within a particular management group, and enables you to identify, diagnose, and resolve problems on the computers within that management group.

The Operator console, which is an application rather than a MMC snap-in, consists of a navigation toolbar and a viewing area. The navigation toolbar includes the menu and command bars, which enable you to navigate, perform various actions, and obtain a quick view of current activity.

Operator Console Real Estate

The main viewing area of the Operator console is divided into four panes that access multiple views, providing you with the information necessary to troubleshoot a problem while staying within a single window.

Operator Console Panes

Many Network Operations Centers (NOCs) maintain a single console with a multipaned view for monitoring computer status and alert notifications simultaneously. The design of

the MOM 2005 Operator console utilizes this approach and divides the real estate of the monitoring window into four separate and distinct areas (see Figure 8.11):

- **Navigation Pane**—Allows you to navigate through the view hierarchy. You can change views by selecting the various navigation buttons.
- **Results Pane**—Appears to the right of the Navigation Pane. When you select a view and then a node in the hierarchy tree, the Results Pane displays, naturally, the results of that selected view.
- **Details Pane**—Appears below the Results Pane. As you select a row (result) in the Results Pane, the contents of the Details Pane change to display the details corresponding to that particular result.
- **Tasks Pane**—Used to launch context-specific actions to help resolve issues or perform tasks from within the Operator console. The tasks you can select vary based on the view you are working with.

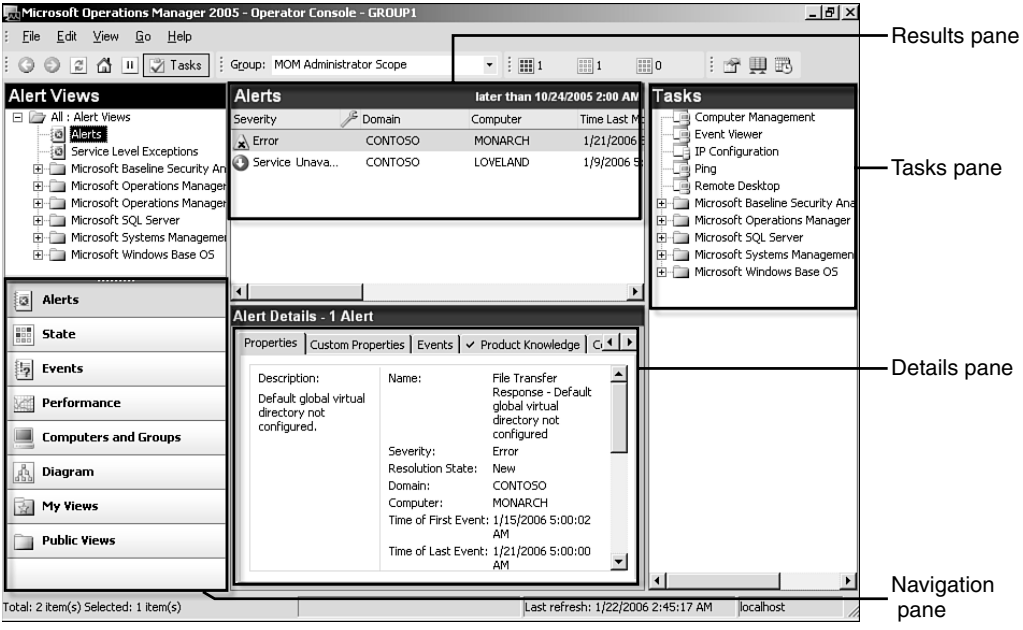


FIGURE 8.11 The viewing panes of the MOM 2005 Operator console.

Views

If you look at the Navigation Pane you will notice that it lists eight view types, as shown in Figure 8.11. As you select a particular view, the other panes in the Operator console change accordingly, and as you drill down on an item in the Results Pane you will go to the next level of detail.

At any time you can limit the scope of what you are viewing by selecting the Computer Group you want to display from the Group drop-down list above the Results Pane. The Group list is actually a means of filtering the data you see. For example, Figure 8.11 uses the MOM Administrator scope as its Group and displays the Alerts view with its corresponding panes.

Alerts The Alerts view is one of the more commonly used views in the Operator console. All open alerts from the computers in the management group are displayed here, with information regarding the severity of the alerts, acknowledgements, and escalation levels.

The data displayed is for all the computer groups in the scope you select. If you are logged on with a user account that is a member of the MOM Administrator group, you see all the data associated with the MOM Administrator Scope.

Data in the Alerts view is displayed using a predefined selection of information displayed in a particular order. You can sort the data by clicking on the column heading you want to sort by. To change the selection of data you see, you can change the view properties, change the data elements by personalizing the columns you see, or change the view time filter. These actions are accomplished by clicking on the appropriate icon on the right-hand side of the Operator console above the Results Pane. MOM Users can select the Personalize View or Edit View Time Filter icons only:

- **Alert View Properties**—Selecting this icon initiates the Alert View Properties Wizard, which steps you through the selection of the type of alerts you want to display. For example, the default is to see only unresolved alerts. You can modify the Alert View Properties to change the view, perhaps to see previously closed alerts and determine how prior problems were resolved.
- **Personalize View**—Choosing this icon displays a screen allowing you to choose which available columns should be displayed, and the order in which to display them.
- **Edit View Time Filter**—Selecting Edit View Time Filter gives you the capability to view information based either within a date and time range or those that have occurred within a specific number of days. By default, only alerts from the past seven days are displayed.
- **State**—This view shows the current state of all the computers within the management group. For each computer, the health of particular components is displayed. The components shown will vary based on the management packs installed for the management group. As you drill down on a particular computer, it opens up the Alerts Pane for that system.

  You can change the State view by selecting either the State View Properties or the Personalize View icons, located above the Results Pane on the right. MOM Users have access to the Personalize View icon only. Figure 8.12 shows the State view.

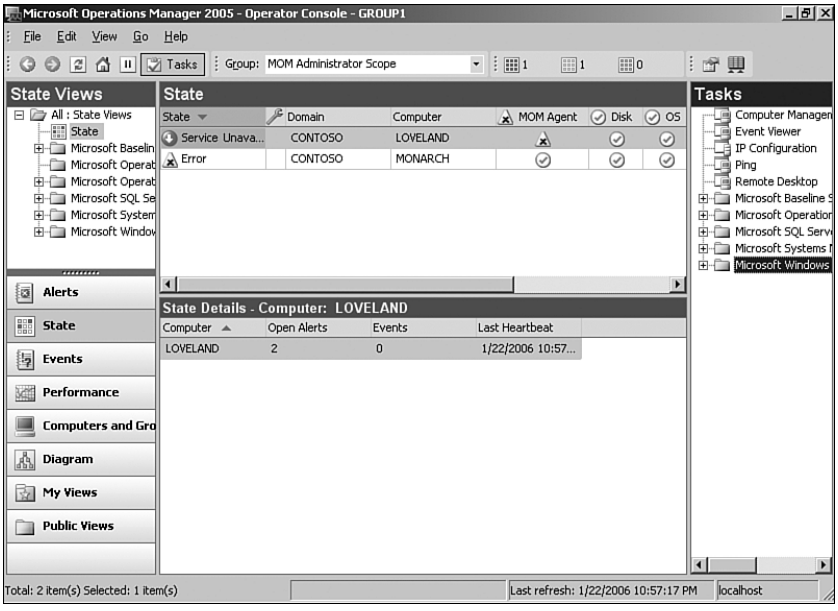


FIGURE 8.12 The MOM 2005 Operator console State view.

Events The Events view consolidates all events that have occurred on monitored systems within the management group. The information is shown in the Results Pane and can be sorted by any column including event type, time, domain, computer, description, source, category, event number, user, or event id. By consolidating event logs, the Operator console provides a central location to search through the error logs when researching a service failure or warning. Figure 8.13 shows the Events view sorted by event type.

MOM Administrators and MOM Authors can customize the Events view by selecting the Event View Properties, Personalize View, or Edit Time View Filter icons above the Results Pane. MOM Users have access only to the Personalize View and Edit Time View Filter selections only.

Performance Two different performance views can be accessed using the Operator console:

- The Performance View lists each computer and the number of performance measurements collected. The specific performance counters sampled are based on the rules in the management packs installed for that management group. There is no Details Pane for the Performance View; selecting one or more computers allows you to choose particular counters to graph real-time or print. This is the default performance view, accessed when you select Performance View in the Navigation Pane.
- The second view is the Performance Data View. This window displays information on performance objects you specify that can include processor, memory, logical disk, or all data in a specified computer group.

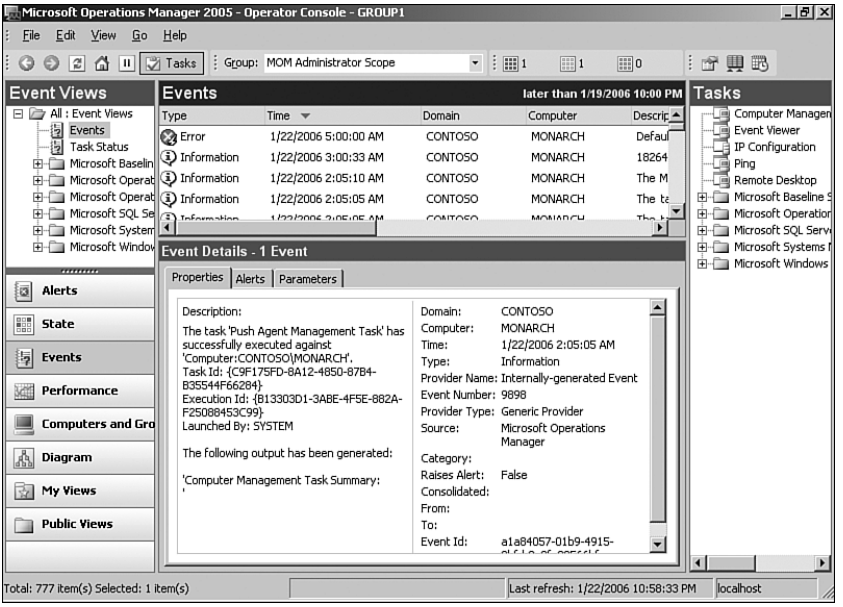


FIGURE 8.13 The MOM 2005 Operator console Events view.

By going to My Views you can create your own Performance or Performance Data view. The view creation process uses wizards to walk you through selecting computers to create a view. The Performance Data View Wizard allows you to select specific counters for viewing as part of the view creation process.

MOM Users are able to select the Personalize View icon only to change the columns displayed in the Performance Results Pane, whereas MOM Administrators and MOM Authors can also customize their view by selecting the Time Filter icon. By default only the last 2 hours of performance data are included.

Computers and Groups Selecting Computers and Groups opens the Computers and Groups View, which allows you to choose from two predefined views—the status of either Computer Groups or Computers.

- The Computer Groups listing shows all installed computer groups, including the state and any open alerts for each. Selecting a particular computer group allows you to drill down for information on computers belonging to that computer group; the console displays the alerts associated with that particular system as you select a specific computer.
- The Computers listing displays the status of each computer that has been discovered, including its state, time of its last heartbeat, number of alerts and errors. The Details Pane allows you to view attributes, rule groups, computer groups, and roles associated with that computer. You can also drill down into an individual computer to view related alerts.

Within the Computers and Groups view, the View Properties and Personalize View icons are available to MOM Administrators and MOM Authors. MOM Users can access the Personalize View icon only, modifying the columns displayed and the order in which they are shown.

Diagram The Diagram view is a graphical representation of the computers and their relationship within the management group, including the green/yellow/red light status of each computer. A graphical diagram represents each computer group identified to MOM, along with its status. The default view shows only the top-level diagram view in the Results Pane. You can zoom in or out, or expand the levels of detail being shown.

Additional Diagram Views

Various management packs provide additional useful diagram views, such as the Exchange and Active Directory management packs.

My Views My Views shows custom views accessible only to the operator who created them. You can create new views by right-clicking on the All My Views folder and specifying a new view of a particular type. A wizard walks you though the steps to create the new custom view.

Members of the MOM Administrators and MOM Authors groups can create new views anywhere in an active view, Public Views, or My Views. MOM Users are limited to creating a new view in My Views only.

Public Views Public Views allows you to display all views accessible to all operators with no view type filtering.

Customizing the Operator Console

The Operator console provides the flexibility to customize its views based on your particular requirements. Your security role and scope—based on the MOM security group to which you belong—determine your flexibility in modifying the console.

A MOM Administrator can specify the computer groups and views to which MOM Operators have access.

Restrictions on Viewing Data

Although all views specified are available, they will not include data from computers not in the scope's list of computer groups.

A computer operator typically belongs to the MOM Users local security group, and as such cannot access any information outside a defined console. This enables you, as an Administrator, to divide operational responsibilities as needed in a single management group.

Computer operators, although they can work only within the scope of a defined console, may be able to target specific data within that console by creating custom views. For instance, an operator might define a custom alert view where he can filter data to see new or unresolved alerts.

To create a new view, a MOM Administrator or MOM Author would perform the following steps:

1. Select the pane for which you want to create a new view, and in the View list, which lies above, right-click on the rule group for which you want to apply the new view.
2. Select New from the drop-down menu, then View, where the View type will be the pane previously selected.
3. This initiates the associated Create New – *xxx* View Wizard, where *xxx* is the specified viewing pane.
4. The wizard walks you through the steps associated with creating the appropriate view.

Installing Consoles on Remote Computers

The Administrator and Operator consoles are initially installed on the management server. One of your tasks after installing MOM is to install consoles on computers used by individuals who monitor operations or maintain MOM. Placing additional consoles on remote computers enhances physical security by limiting direct access to the production management server. Additional consoles also make monitoring more convenient for the individual sitting at his or her desk.

To install a console remotely, the intended system must be running Windows 2000 Service Pack 4 or later, Windows XP Professional (or 64-bit with Service Pack 1), or Windows Server 2003; the Microsoft .NET Framework 1.1; and have at least 128MB of RAM available. The consoles are installed by running the MOM 2005 Setup program setup.exe, located in the root of the MOM installation directory, on the computer you will be installing the consoles to, and specifying a custom installation. The specific procedure follows:

1. In the MOM Setup menu, select the option to Install Microsoft Operations Manager 2005, and because you are installing the consoles only, choose a custom installation, as illustrated in Figure 8.14.
2. On the Custom Setup screen (see Figure 8.15), make sure that the only component selected for installation is the MOM 2005 User Interfaces.

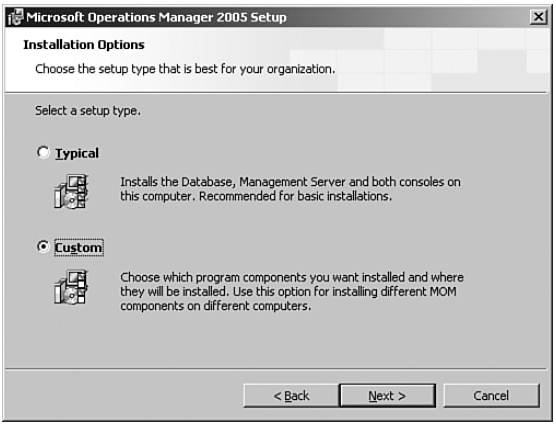


FIGURE 8.14 Choose a custom installation to install the consoles only.

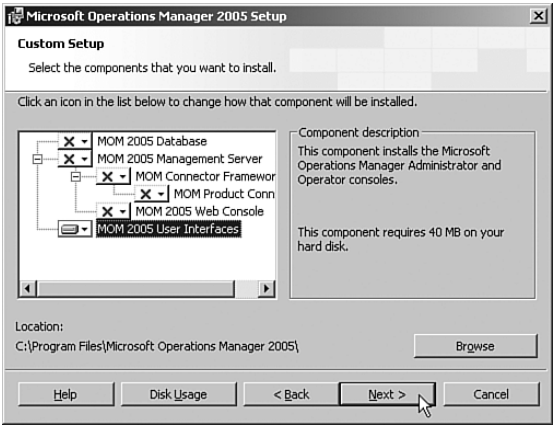


FIGURE 8.15 Check that the only component to be installed is the MOM 2005 User Interfaces.

3. After passing the prerequisite check, you are prompted for the name of the management server as shown in Figure 8.16.
4. To complete the process, click Next to install the Operator and Administration consoles.

If the MOM web interface or MOM Reporting are installed, those consoles may be accessed from any computer using Internet Explorer 5.5 or a later version of the browser.

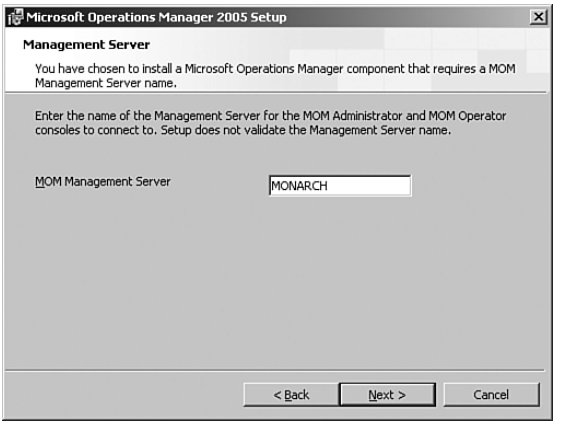


FIGURE 8.16 Specify the name of the management server.

MOM 2005 Reporting

If you install MOM Reporting, there are several tasks to consider for maintaining the reporting server. These include sizing, configuring Data Transformation Services (DTS), and grooming.

Sizing MOM Reporting

As mentioned in Chapter 4, "Planning Your MOM Deployment," there is a direct relationship between the size of the MOM operational database and the MOM reporting database. To estimate the size for the MOM reporting database, determine the growth of OnePoint for one day, and multiply for the number of days of retention, which we discuss in the "Grooming the Reporting Database" section later in this chapter. You should then double that number to account for indexes. This calculation is represented by the following formula, which was provided in Chapter 4:

```
(Size of data/day x Retention Days) x 2 = SystemCenterReporting Database
```

Impact of Adding More Data to OnePoint

If you increase the amount of data reported to the MOM database by adding new management packs or monitoring additional computers, the size of the reporting database also increases.

The log file for SystemCenterReporting should be the size of one day's growth and multiplied by five to account for indexes. The tempdb on the SQL Server instance containing OnePoint must be large enough to accommodate one day's growth for that database.

Configuring DTS

MOM runs a nightly task to transfer data from OnePoint to SystemCenterReporting. This task runs by default at 1:00 a.m. If you change the schedule, be sure it will not run while the grooming task is running—that causes the DTS job to fail.

To change the schedule for the transfer job, perform the following steps on the MOM reporting server:

1. Using an administrative account, use the Start menu to navigate to Accessories / System Tools / Scheduled Tasks.
2. Double-click the *SystemCenterDTSPackageTask*.
3. On the Schedule tab, set the start time and frequency for the job to run.

The DTS job may fail if the SystemCenterReporting transaction log fills up before being able to do a checkpoint. This situation can be alleviated by running the DTS job manually, using the /latency switch to control the number of days of data being moved. To run the DTS job such that all data older than 30 days will be moved, use the following syntax:

```
MOM.Datawarehousing.DTSPackageGenerator.exe /latency:30 /srcserver:OnePointDBServer
/srcdb:OnePoint /dwserver:WarehouseServer /dwdb:SystemCenterReporting
/product:"Microsoft Operations Manager"
```

Start with a "big" number and work your way down to four days, which is the default retention period for the OnePoint database. A complete list of options and syntax for the DTSPackageGenerator follows:

```
DTSPackagegenerator.exe <Options>
Options:
/product Product name (Default=Microsoft Operations Manager)
/srcserver Source server name (Default=.)
/srcdb Source database name (Default=OnePoint)
/dwserver Datawarehouse server name (Default=.)
/dwdb Datawarehouse database name (Default=SystemCenterReporting)
/savetodisk Indicates package save (Default is do not save)
/savepath Path to save (Default=)
/donotrun Indicates do not run (Default is to run)
/dwserver Datawarehouse server name (Default=.)
/dwdb Datawarehouse database name (Default=SystemCenterReporting)
/savetodisk Indicates package save (Default is do not save)
/savepath Path to save (Default=)
/donotrun Indicates do not run (Default is to run)
/silent Indicates to hide the console window (Default is to show)
/maxconn Max connections, controls how many steps can run in parallel (Default=8,
MinimumRequired=5)
```

```
/latency Latency in days, indicates how much latency (in days) to subtract from the
current UTC date while computing the high watermark. All rows that satisfy (Current
UTC date - latency) are transferred (Default=0.00347222222222222222222222 [5
minutes])
/chunksize Chunk size in days; high volume data will be transferred in increments
of the chunk size, thereby enabling transfer of high volume data with limited log
space. Specifying 0 will not chunk the data (Default=1 day)
/maxchunks Maximum number of chunks to create when chunking is enabled (Default=10
chunks)
/usesqlauth Indicates use SQL Authentication; SQL Authentication should not be used
(Default is to use Windows Authentication)
/srcsqllogin Source SQL Login; used to connect to source database. Used only for
SQL Authentication, which should not be used
(Default=)
/srcsqlpwd Source SQL Password, used to connect to source database. Used only for
SQL Authentication, which should not be used (Default=)
/dwsqllogin Warehouse SQL Login, used to connect to warehouse database. Used only
for SQL Authentication, which should not be used
(Default=)
/dwsqlpwd Warehouse SQL Password, used to connect to the warehouse database. Used
only for SQL Authentication, which should not be used (Default=)
```

Some of these options were added with MOM 2005 SP1.

Grooming the Reporting Database

In the "Scheduled MOM Database Maintenance Tasks" section earlier in this chapter, we discussed grooming the MOM database. You can also groom the reporting database to change the retention time for data used with MOM Reporting.

The MOM Reporting installation creates the *p_updategroomdays* stored procedure in the SystemCenterReporting database. By default, the data in the MOM database that is archived to the reporting database is retained for 13 months (395 days). To modify the retention period, create an SQL Server query on the MOM reporting server similar to the following example, substituting values for `TableName` and `DaysToRetainData`:

```
Use SystemCenterReporting
go
Exec p_updategroomdays 'TableName', DaysToRetainData
```

`TableName` is one of the six main tables in the SystemCenterReporting database, and `DaysToRetainData` is the number of days to retain data in the specified table. You will want to run the query for each of these tables:

- `SC_AlertFact_Table`
- `SC_AlertHistoryFact_Table`

- SC_AlertToEventFact_Table
- SC_EventFact_Table
- SC_EventParameterFact_Table
- SC_SampledNumericDataFact_Table

The table name must be in single quotes. For example, you would use the following query to retain data in the SC_AlertFact_Table for 150 days:

```
Exec p_updategroomdays 'SC_AlertFact_Table', 150
```

Sizing and grooming the SQL Server databases have an impact on performance. More information on performance can be found in Chapter 10, "Complex and High Performance Configurations."

Summary

This chapter discussed the functions and components of the MOM consoles, stepping through the process to install consoles on remote machines. We used wizards to install agents and management packs. We introduced console scopes and security groups, and discussed their functionality within the Administrator and Operator consoles. We also discussed maintenance tasks for the MOM operational database, and the process of sizing and grooming the reporting database.

It is now time for an in-depth discussion of agents, which is the topic of the next chapter.

This page intentionally left blank

CHAPTER 9

Installing and Configuring Agents

IN THIS CHAPTER

This chapter focuses on agents and how they are used in Microsoft Operations Manager (MOM) 2005. We discuss what agents are and how MOM discovers computers and deploys agents. We explain the differences between agent-managed and agentless-managed computers and the concepts of unmanaged computers and multihomed agents. Finally, we discuss how to manage agents, including how to remove agents from the systems in your environment.

Understanding Basic Concepts

Several core concepts, such as the discovery process and the approval process, are relevant to understanding how agents function with MOM 2005. In addition, a monitored server can exist in one of three management states: agent-managed, agentless-managed, and unmanaged. An agent-managed system can also be multihomed, meaning that it is managed by multiple management groups, which is described in the "Multihomed Agents" section later in this chapter. The following section explains various terms and their meanings.

Discovery Process

MOM 2005 uses a *discovery* process to identify systems on which you can install agents or systems you can configure for agentless monitoring. This discovery process queries the Active Directory directory service for computer information matching the requirements defined for the discovery process. Machines residing in nontrusted domains and workgroups can be discovered if the computer name is provided in the format of Domain\ComputerName or Workgroup\ComputerName.

Approval Process

Although agent installation can take place automatically after a system is discovered, by default MOM 2005 utilizes an approval process before an agent is installed on a discovered system. The *approval process* enables the MOM administrator to control which specific computers receive the agent. Systems requiring approval are placed in the Pending Actions folder, which is located in the MOM 2005 Administrator console under Administration \ Computers \ Unmanaged Computers.

You can enable Automatic Management for a single management server (allowing the management server to automatically install, uninstall, or upgrade agents) in the Administrator console. Perform these steps:

1. Navigate to Administration \ Computers \ Management Servers.
2. Right-click on the management server(s) and select Properties.
3. Click on the Automatic Management tab and uncheck the Use Global Settings option.
4. Choose to automatically install, uninstall, and upgrade agents and automatically stop and start agentless management."

Agent-Managed State

An *agent-managed* system runs a software component called the MOM *agent*, which runs as a local service on the computer on which it is installed. The agent monitors the computer using the management pack rules applying to that agent. These rules are updated by the management server when changes are applied to management packs used by that system. Updated rules are received by the agents at the next request configuration interval (defined under Administration \ Global Settings \ Agents \ Configuration Requests) after changes are applied. Typically, MOM configurations are based on agent-managed systems.

The MOM 2005 setup process installs only the MOM management pack, so initial information gathered from agent-managed servers is based on the rules in that management pack, pertaining to the health and availability of the MOM agent. As other management packs are integrated into MOM 2005, additional items are monitored depending on the function of the server.

MOM 2005 agents can be deployed to the following operating systems:

- Microsoft Windows 2000 Server family Service Pack 3 (SP3) and later
- Microsoft Windows Server 2003
- Microsoft Windows XP Professional

Monitor Windows XP Professional with MOM

Although Windows XP Professional can be monitored by MOM, typically organizations only monitor servers. An exception to this rule might be a batch processing system that runs business-critical functions that has not been migrated to a server platform.

For example, many manufacturing companies use workstation-class computers to monitor machines that produce their products.

Microsoft Windows NT 4.0 is not supported in an agent-managed configuration. If it is necessary to manage Windows NT 4.0 systems, either consider agentless management or review third-party supplemental packages for MOM 2005.

Desktop Base Operating System Management Pack

Microsoft provides the Desktop Base Operating System Management Pack to monitor the performance and availability of Windows XP and later desktop versions of the Windows operating system. You can download the Desktop Base Operating System Management Pack from http://go.microsoft.com/fwlink/?LinkId=50270. For more information about monitoring desktop operating systems, see the *Microsoft Windows XP Professional Resource Kit*, Third Edition (Microsoft Press, 2005).

Agentless-Managed State

An *agentless-managed* system does not run the MOM agent. The agent component on the management server collects data from the agentless-managed computer in this configuration through remote calls to the managed system. MOM 2005 supports only up to 10 agentless-managed systems reporting to a management server. Agentless systems are actually monitored from the management server itself and increase the load on that management server. The limitation of 10 agentless systems reporting to a management server is the maximum *supported* configuration, but additional agentless systems could be added to your management server, based on your hardware configuration. Additional information regarding the performance impact of agentless monitoring on the management server is available in the "Results for Agentless Monitoring" section of the MOM 2005 Performance and Sizing Guide, available at http://go.microsoft.com/fwlink/?linkid=47141.

Sometimes, application owners are concerned about the installation of agent software onto their application servers and the impact that it might have on the operations of that computer. The resource load on an agent-managed computer is low and usually does not pose a problem. However, in some environments any change to the configuration or installed software base leads to complications. In some cases, the Information Technology (IT) group responsible for server management wants to avoid even the appearance of impacting an application server, thus avoiding potential liability. In these cases, the agentless management mode can give the organization management of servers that might otherwise be unmanaged. (Because Windows NT 4.0 systems do not support a MOM 2005 installed agent, you will have to use agentless monitoring if you need to monitor those systems.)

Agentless-managed computers have a more limited set of features than do agent-based managed computers. Similar to agent-based managed computers, agentless-managed computers have the following features:

- State monitoring
- Heartbeat

- Service discovery
- Performance collection
- Script execution
- Event collection

Limitations with Agentless Systems

Limitations with agentless-managed systems are described in the "Integrating Agentless-Managed Systems into MOM 2005" section later in this chapter.

Unmanaged State

Unmanaged systems are those that have been identified for potential management in the future or that have been taken offline for reasons such as long-term maintenance. No information is gathered from unmanaged systems.

Discovering Computers and Deploying Agents

Discovering computers and deploying agents are key steps in integrating servers into MOM 2005. This section describes computer discovery rules, how to customize the computer discovery process, and the steps involved in agent installation.

Install/Uninstall Agents Wizard

The Microsoft-recommended way to discover and install agents is by using the Install/Uninstall Agents Wizard. This wizard is available in the Navigation pane of the Administrator console on the Microsoft Operations Manager home page or by right-clicking the Computers folder under Administration and selecting the Install/Uninstall Agents Wizard.

The wizard enables you to browse for specific computers and also creates the computer discovery rule for you. Details on how to create discovery rules separate from this wizard are discussed in the next section. The wizard itself is discussed in more detail in the "Deploying Agents" section later in this chapter.

Configuring Discovery Rules

If you want to add systems into MOM independent of the Install/Uninstall Agents Wizard, the first phase in integrating systems into MOM is to configure discovery rules to make those computers known to MOM. When discovered, systems can be assigned to the states of agent-managed, agentless, or unmanaged.

Listing Unmanaged Computers

Why would you discover a computer and put it in an unmanaged state? Maintaining a list of unmanaged computers provides an easy way to track computers you intend to manage in the future.

Creating Discovery Rules

To become familiar with the process of creating discovery rules, let's look at the process of installing a MOM agent on a domain controller named Loveland in our Contoso.com domain. The management server in this environment is Monarch.

To create discovery rules, complete the following steps:

1. Open the MOM 2005 Administrator console.
2. In the console tree, open Administration \ Computers \ Computer Discovery Rules. The Details pane lists discovery rules that are already defined.
3. In the console tree (Navigation pane), right-click Computer Discovery Rules and choose Create Computer Discovery Rule, as shown in Figure 9.1.

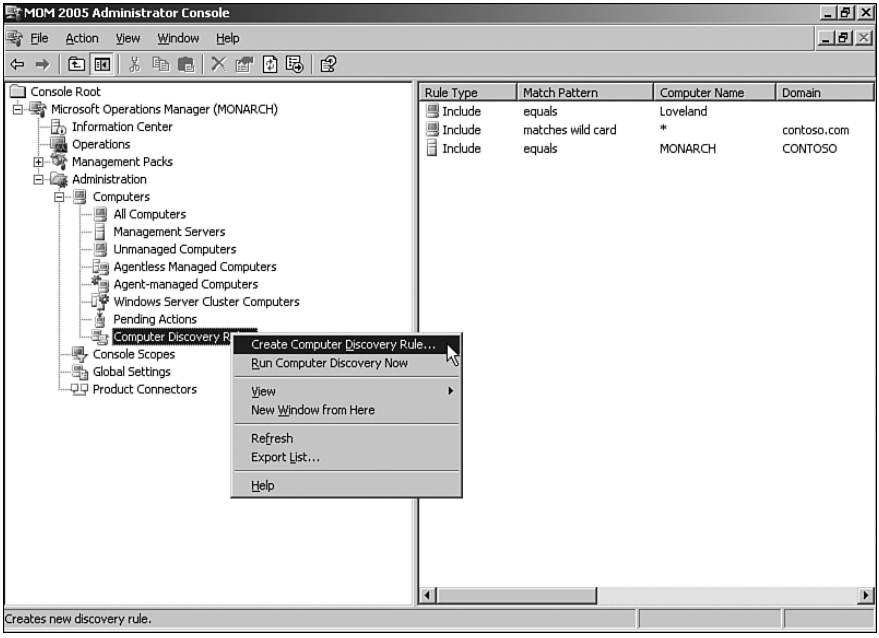


FIGURE 9.1 Creating computer discovery rules.

4. On the Computer Discovery Rule page, provide the following information:

   - Management Server—The default is the current management server to which you are connected. You can choose any other management server already installed in the management group, as happens in configurations with load-balanced agents across management servers. For our example, select Monarch.
   - Rule Type—The default for discovering a system is Include. Exclude is used to specify systems not to be discovered by MOM 2005. Select Include.
   - Domain Name—Use either the NetBIOS name or the fully qualified domain name (FQDN) of the system. Type **contoso.com** in the text box.
   - Computer Name—In the text box to the right, provide the text for the computer name based on the option you select from the list on the left. Select Equals and then type **loveland** in the text box.
   - Computer Type—The options of Server, Clients, and Servers and Clients are available. Select the default, which is Servers and Clients.
   - Initial Management Mode—The options are agent-managed, agentless-managed, or unmanaged. Select Agent-managed, which is the default.
   - Apply Query Criteria To Domain Controllers—This check box indicates whether domain controllers should be included in the results of the query. Because Loveland is a domain controller, select the check box to include domain controllers in the discovery criteria.
   - During Computer Discovery, Contact Each Computer To Verify That It Exists. This check box indicates whether the computer's existence should be verified before adding it to the discovery list. Select this check box if the rule type is Include; this is the default. Clear the check box if the rule type is Exclude. For this example, select this check box.

Name Check Details

The actual verification process is done by executing a forward lookup on the computer name using the Domain Name System (DNS) and then calling the standard Windows application programming interface (API) using NetServerGetinfo. This API requires at least domain user access to the box, and the call determines the computer description and computer type.

Your dialog box should now look like the dialog box shown in Figure 9.2.

5. Click OK to define your discovery rules and close the dialog box.
6. In the Navigation pane of the Administrator console, right-click Computer Discovery Rules and choose Run Computer Discovery Now.

The discovered computers will appear momentarily in the Unmanaged Computers folder until the MOM agent is installed and begins communicating with the management server. After the agent is installed the computer appears in the Agent-managed Computers folder.

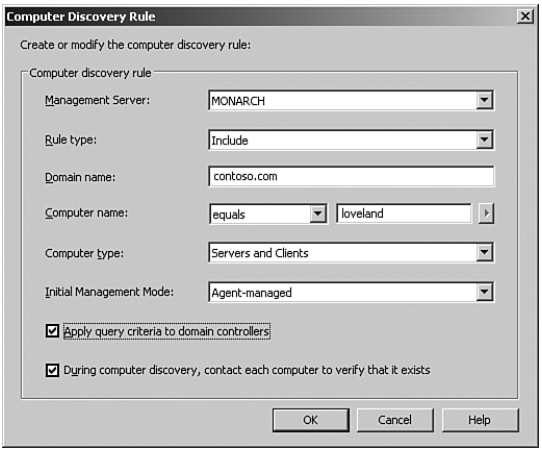


FIGURE 9.2 Specifying the details for a computer discovery rule.

Deleting Discovery Rules

Computer discovery rules should be removed when computer systems that are discovered by a rule either no longer exist or are no longer monitored by MOM. If automatic management is enabled, computers that are no longer discovered will have the MOM agent automatically uninstalled.

To delete discovery rules, complete the following steps:

1. In the Administrator console, open the Computer Discovery Rules folder. In the details pane is a list of the currently defined discovery rules.
2. Right-click the rule you want to delete, and choose Delete from the context menu.
3. Click Yes when you receive the message Are You Sure You Want To Delete The Selected Computer Discovery Rule?

Removing Discovery Rules

When you remove the discovery rule from a server you do not want managed, you prevent MOM from rediscovering the system and attempting to reinstall the MOM 2005 agent.

The default uninstall delay is 48 hours, meaning that the agent is actually removed 48 hours after computer discovery is run. Computer discovery runs every 24 hours. The

uninstall delay is used when computer discovery is run with the computer verification option checked. When the option is checked and a machine cannot be contacted during discovery the computer is marked for uninstallation, which occurs after the uninstallation delay of 48 hours.

By default MOM automatically runs discovery at 2:05 a.m., or you can manually run it in the Administrator console under Administration \ Computers \ Computer Discovery Rules by right-clicking the icon and selecting Run Computer Discovery Now. To force an immediate uninstall of the agent, see the "Removing Agents Manually" section later in this chapter.

Discovering Computers

As previously mentioned, computer discovery rules run by default every day at 2:05 a.m. This setting can be changed at Administration \ Global Settings \ Discovery by inserting a different time in the Run Computer Discovery Time box. You can decrease the frequency from running once a day to running once every seven days (the maximum setting) by altering the Interval For Computer Discovery option in this window.

ManualMC.txt

In addition to using the computer discovery rules discussed in the preceding section, MOM 2005 can use the ManualMC.txt file to discover systems. To have systems discovered, add their names to the ManualMC.txt file and save the file as ANSI (default), Unicode, or UCS Transformation Format 8 (UTF-8) encoded.

Names can be formatted as NetBIOS names, FQDNs, or in the *Domain Name**Computer Name* or *Workgroup Name**Computer Name* format. Enter one system name per line, and do not allow any blank lines in the file. This file must be placed in the MOM install directory, which is *%ProgramFiles%*\Microsoft Operations Manager 2005 by default. ManualMC always installs these systems as agent-managed, not agentless. The computers will be discovered when the next full computer discovery is executed.

Automatic Management

Automatic management specifies whether agents should be automatically installed, uninstalled, or upgraded. Automatic management also specifies whether agentless management should be automatically started or stopped. The default configuration is disabled for automatic management. This configuration is set within the Administrator console under Administration \ Global Settings \ Management Servers, in the Automatic Management tab.

If automatic management is enabled, MOM automatically installs the agents to discovered computers. If automatic management is disabled, MOM places these systems in the Pending Actions folder.

Deploying Agents

Now that you have stepped through the process of discovering computers in your environment, let's look at the tasks associated with deploying an agent, deploying an agentless configuration, and changing an agentless-managed system to an agent-managed system.

Deploying Agents

When you deploy multiple MOM agents, deploy them outside of peak business hours to minimize the impact on network performance. A phased deployment of MOM agents can also help decrease the network impact.

Deploying Agents Using the Administrator Console

Agents can be deployed (pushed) to systems that are located in the Unmanaged Computers folder. This folder is located in the MOM 2005 Administrator console under Administration \ Computers \ Unmanaged Computers. The steps required are as follows:

1. In the Unmanaged Computers folder, click the computer on which you want to install an agent, and choose Install Agent from the drop-down list. This starts the Install Agents Wizard.

Deploying the Agent to Multiple Systems

To deploy the MOM agent to multiple systems, select the systems to be upgraded, right-click the group and choose All Tasks; then select Install Agent.

2. Figure 9.3 shows the Agent Installation Permissions page, where you can specify the Management Server Action Account or give another domain\user name and password with local administrative-level permissions on the remote computer.

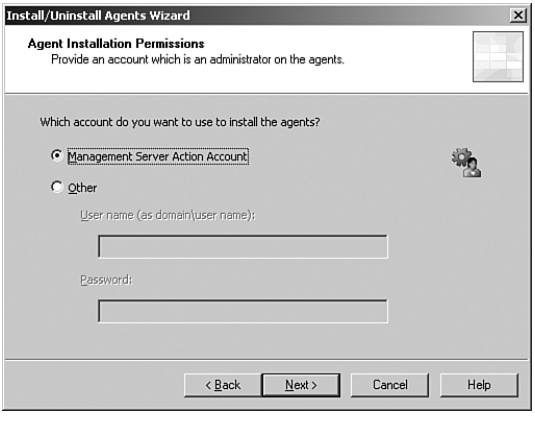


FIGURE 9.3 The Agent Installation Permissions page.

3. At the Agent Action Account page shown in Figure 9.4, you can choose to install using the Local System account or specify a user account and password. See Chapter 11, "Securing MOM," for more information regarding the Agent Action account requirements and required access privileges.

Security Alert

Potential security concerns associated with using the Local System account are discussed in Chapter 11.

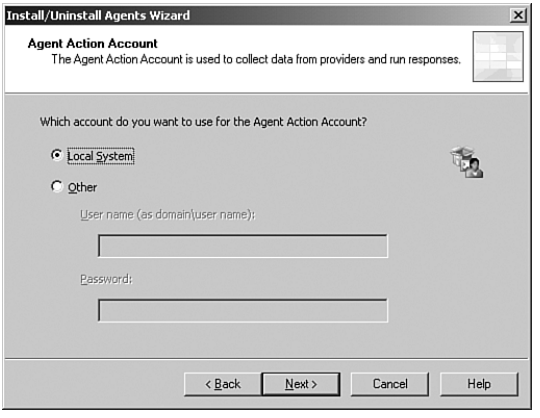


FIGURE 9.4 The Agent Action Account page.

4. On the Agent Installation Directory page you can accept the default installation directory of *%ProgramFiles%*\Microsoft Operations Manager 2005 or enter another installation directory.

5. On the last page of the Install Agent Wizard, the Show Task Progress check box is selected by default. Click Finish to complete the wizard.

   As the install task runs, the Microsoft Operations Manager Task Progress window is displayed. You can click Details to see the status of the installation process, which is shown in Figure 9.5. The process status starts as Running and when completed is categorized as either Succeeded or Failed. If the installation shows a failed state, select a computer on the list, and review the information under Selected Computer Details for the error details.

Real World—Agent Installation Gotchas

Before installing agents, check for some potential trouble spots:

- Permission errors are a common source of failure messages when deploying agents. If the agent installation fails because of a permissions error, verify that the account you are using has local administrative access to the system to which the agent is being deployed.
- Windows Installer 3.1 must be deployed on the system for the MOM 2005 SP1 agent to install. The Windows Installer is available from Windows Update (www.microsoft.com/windowsupdate) or the Microsoft Download Center (http://www.microsoft.com/downloads) and should already be installed on systems if patch management is current.

6. After the installation process completes, close the MOM Task Progress window and refresh the Unmanaged Computers folder view. The system on which you installed the agent no longer appears in the Unmanaged Computers view and now appears in the list in the Agent-Managed Computers folder.

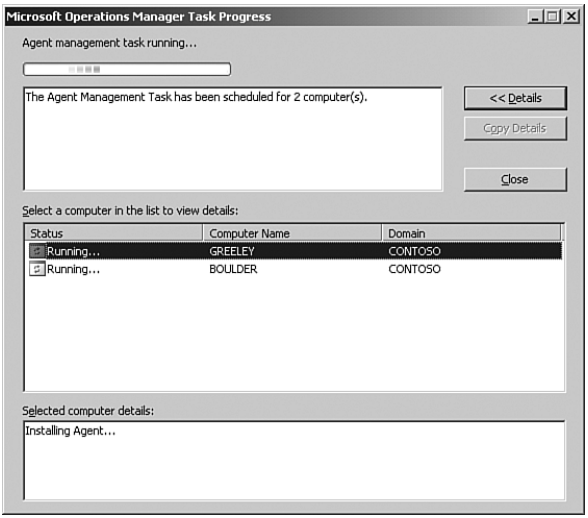


FIGURE 9.5 The Microsoft Operations Manager Task Progress screen.

Agents and Firewalls

There are specific networking requirements when deploying agents from the MOM Administrator console to a targeted system. The management server needs specific ports open to communicate, and it must resolve the name of the target system with the correct Internet Protocol (IP) address.

MOM uses Server Message Blocks (SMB; TCP/UDP port 445 + the entire DCOM port range) and remote procedure calls (RPC; TCP port 135) to deliver the files used to install the agent. These ports must be open on both the management server and the target system. The agent must be installed manually if one of the following conditions is true:

- The ports are blocked on the client side (in the case of the Windows XP SP2 or Windows Server 2003 SP1 firewall).
- The ports are blocked on the server side.
- There is a hardware firewall between the target computer and the management server.

For those Windows systems using the Windows firewall, Microsoft knowledge base article 885726 (http://support.microsoft.com/kb/885726/) discusses the Windows firewall and registry configuration changes necessary on the target system to resolve this issue. Additionally, ISA Server 2004 notes port 445 as used by the Sasser worm. Blocking TCP port 445 in the outbound direction prevents outbound Internet File System (CIFS) traffic from working across ISA Server.

Additional information on ports to be configured when using MOM 2005 in a firewall environment is documented in Chapter 11 and in the Microsoft Operations Management 2005 Security Guide at http://go.microsoft.com/fwlink/?linkid=50271.

Manual Agent Installation

The manual agent installation process is another method for installing MOM 2005 agents. Some configurations require manual installation of the agent, including when any of the following occur:

- The system is behind a firewall.
- Bandwidth limitations on the connection to the management server prevent automatic installation.
- A highly secured server configuration is required.

Enabling Manual Agent Installation

In a freshly installed MOM 2005 environment (not upgraded from MOM 2000), you must configure the management server to allow new agents to be installed manually. Manually installed systems are considered to be *unauthorized* agents. The default configuration prevents unauthorized agents from being installed automatically.

To configure manual agent installation, navigate to Administration \ Global Settings \ Management Servers. On the Agent Install tab, the Reject New Manual Agent Installations option must *not* be selected if you want to allow manual installation of agents. If you change this option, you must right-click the Management Pack folder, click the Commit Configuration Change option, and then restart the MOM service on all management servers in the management group to apply the change.

Before attempting to install a MOM agent manually, start the MOM 2005 Administrator console. In the navigation pane select Computers and then open Unmanaged Computers. If the system requiring manual installation is listed or if a previous push install has failed, right-click the system and choose Delete. Next, right-click the Management Pack folder and select the Commit Configuration Changes option.

The installation process should take place on the computer where the agent will be installed. To install a MOM agent manually, complete the following steps:

1. Run Setup.exe to start the Agent Setup Wizard. Setup.exe is available on the Microsoft Operations Manager 2005 installation media.

Another Way to Install the Agent

The agent can also be installed by running the MOMAgent.msi file that is stored in the I386 directory on the MOM 2005 installation CD or in the *%ProgramFiles%*\Microsoft Operations Manager 2005\x86 directory structure on the management server. The installation process should take place on the computer where the agent will be installed.

2. In the MOM 2005 Setup Resources window, click the Manual Agent Install tab and click the Install Microsoft Operations Manager 2005 Agent option.
3. In the Agent Setup Wizard, select the default destination folder and click Next to continue. Figure 9.6 shows the Agent Configuration page.
4. Enter configuration information for the Management Group Name, Management Server, Management Server Port (the default port is 1270), and Agent Control Level (None or Full) options. Additional management servers can be specified by clicking Advanced and identifying the servers in the Advanced tab.

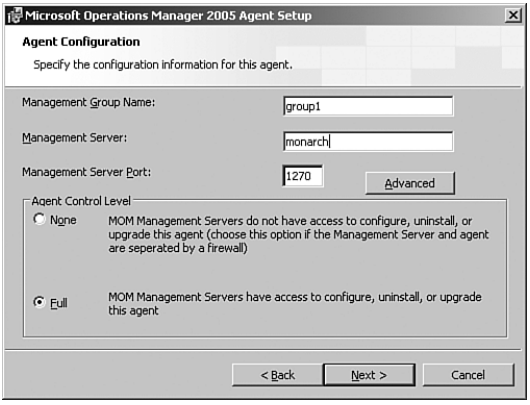


FIGURE 9.6 Specifying the configuration information for an agent.

5. Select an Agent Control Level option from the two possible configurations:
   - None—The management server does not remotely upgrade, apply patches, or uninstall agents. Upgrades, patches, and uninstallation must be done manually. Configuration and rule updates are still applied.
   - Full—The management server performs all operations for the client, including agent configuration, patch application, upgrade, agent uninstallation, and attribute collection. This option is the most effective choice when managed computers exist on your internal network.
6. Click Next to continue. The MOM Agent Action Account defaults to Local System or can be configured to use a domain or local account. If you do not use Local System, the Action Account requires at least local Administrator group-level permissions.

Security Information

See Chapter 11 regarding security requirements for the Agent Action Account.

7. On the Active Directory Configuration page shown in Figure 9.7, choose either Yes or No to indicate whether the management server is in a trusted Active Directory domain. Note that this setting must match the global setting for the management group regardless of whether the management server is in a trusted domain.

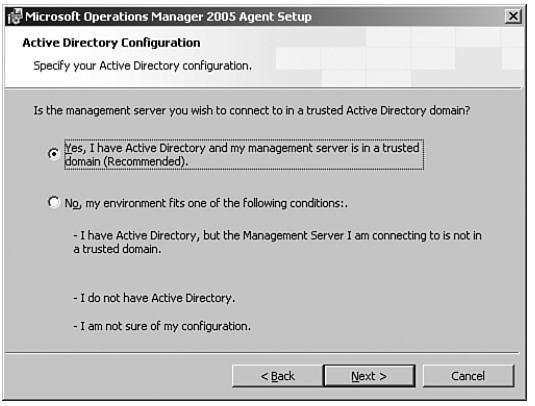


FIGURE 9.7 Specifying the Active Directory configuration relationship for the Management Server.

8. Continue to the Ready to Install page where you will verify your configuration and then start the installation.

If the manual installation is successful, the computer is shown in the Agent-Managed Computers list. If the installation fails, the system remains in the Unmanaged Computers folder.

Configuring Agent-Managed Systems

Some configuration changes may need to be made on agent-managed servers, depending on how many events are logged on the server and what operating systems are monitored. These changes include the following:

- Event log configurations
- Disk performance configurations

Event Log Configurations

The event logs of the monitored systems provide one of the major data sources for MOM. If the event log on a managed computer fills completely, event logging either stops or events are overwritten depending on the configuration of the event log. A full security log can even stop the computer from functioning! If the event log cannot gather information, MOM cannot provide information effectively about the status of the monitored system.

Security Alert

If the security log on a managed computer fills up, the managed computer can lock up. Refer to knowledge base article 232564 on the Microsoft Help and Support website for details on this issue. This article can be located at http://support.microsoft.com/kb/232564/.

The recommended log file configuration for managed systems is to increase the size to a maximum of at least 25MB and to configure the logs to overwrite events as needed for all event logs, including the NT event logs (application, security, and system) and other event logs such as the Directory Service, File Replication, and DNS logs.

Configuring the Event Logs

You will want to configure your event logs such that you can capture all the events to be sent to the management server:

- Configure your event logs to overwrite events as needed. This ensures that even if the event log fills, it will continue to log new events by overwriting older ones, and it will prevent the logs on managed systems from filling up and stop logging event information.
- Caution! Setting a security log to overwrite events as needed can result in loss of security event information. Refer to your company's security policy regarding event logging before changing this configuration.
- Increase the size of the log files on monitored computers to enable MOM to gather event log information successfully. If additional disk space is available, it is recommended you further increase the size of the logs especially if the system generates large amounts of data in a particular log. (This typically occurs on domain controllers or for applications that log large amounts of data.)

The log file settings for a system can be modified by clicking Start, pointing to Programs or All Programs, clicking Administrative Tools, and then clicking Event Viewer (or click Start, click Run, type **eventvwr** in the Open box, and click OK). Right-click the first event log you want to modify, and click Properties. Modify the Maximum Log Size and Overwrite Events As Needed options. Each log must be set individually using this method.

Methods to Configure Event Logs Settings

You can use several other techniques for changing the settings for the event logs. These include the following:

- Using the ConfigureEventLogs Utility
- Using a Group Policy Object (GPO)

The ConfigureEventLogs utility from the MOM 2000 Resource Kit enables you to automate the process of setting the event log configurations based on an input file listing the server names. This tool is *not* supported by Microsoft and is available only as part of the MOM 2000 Resource Kit. This and other MOM 2000 Resource Kit utilities are available for download at http://go.microsoft.com/fwlink/?linkid=36078.

If the majority of your systems are integrated with Active Directory, a more effective approach to changing these configurations might be by creating a GPO to maintain these settings. The recommended approach is to move all servers (do *not* move the domain controllers) into an organizational unit (OU) and apply the GPO to that OU. Figure 9.8 shows an example of how this GPO might be configured.

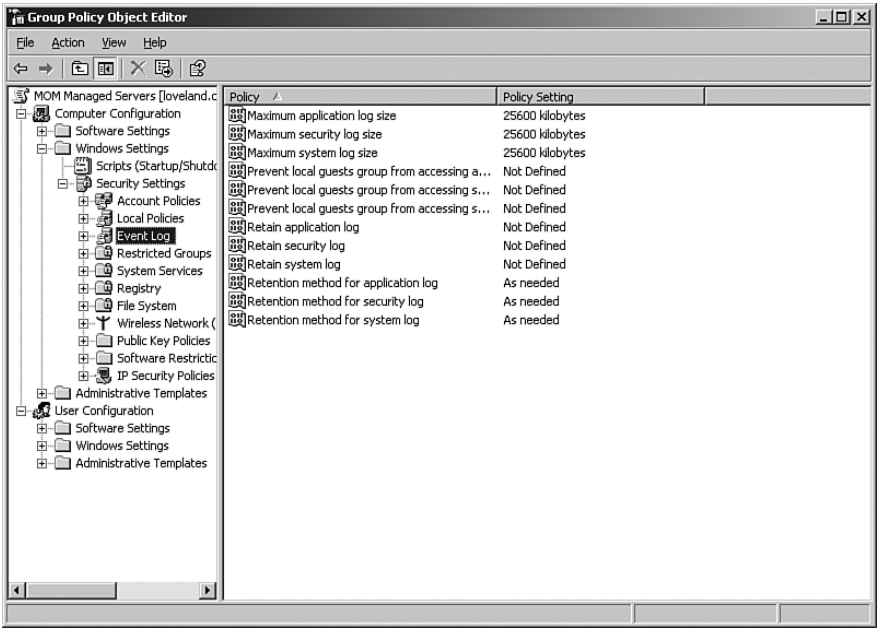


FIGURE 9.8 Sample GPO for event log size and retention method for MOM-managed servers.

Using a GPO can save you work through automating the configuration of the application security and system log settings for all servers in that OU. A similar GPO can be applied to the Domain Controllers OU to change domain controller settings. Note that these GPO examples configure only the application, security, and system logs settings. Additional logs must be modified manually.

Disk Performance Configurations

To gather disk performance information, make sure that each system with an installed MOM agent has its disk performance counters activated. Activate the performance counters by using the command `diskperf -YV`; this takes effect after a reboot. In Windows 2000, the physical disk counters are turned on by default, but the logical disk counters are turned off by default. In Windows Server 2003, both the physical and logical counters are permanently enabled.

Multihomed Agents

Agents that belong to multiple management groups are known as *multihomed agents*. Multihomed agents provide data to multiple management groups. There are some installation steps specific to multihomed agents, which we will discuss first.

Configuring Multihomed Agents

Multihomed agents can be installed (pushed) either by running the Install/Uninstall Agents Wizard (discussed in the "Install/Uninstall Agents Wizard" section earlier in this chapter) for each management group, or manually by running the MOM Agent Setup Wizard on the managed computer.

Manually installing an agent on a multihomed system requires different steps. These include

1. Open the Add/Remove programs and click on Change as shown in Figure 9.9.

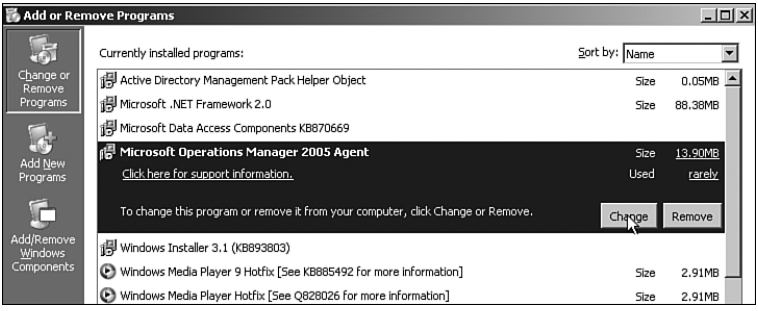


FIGURE 9.9 Installing a multihomed agent through Add/Remove Programs.

2. The Welcome screen of the wizard is displayed; click Next to continue.
3. Because a MOM agent was previously installed on the system, the Program Maintenance screen is displayed with options to Modify, Repair, or Remove the agent. If you needed to repair the MOM agent or manually remove the agent, those options are available on this screen. To configure the agent to connect to another management group choose the option to Modify as shown in Figure 9.10.
4. On the Manage Agent Management Groups screen options are available to Add, Remove, or Modify a Management Group. These options provide a way to add, remove, or modify the agent for a specific management group. Choose Add Management Group as shown in Figure 9.11.

FIGURE 9.10 Modify, repair, or remove the MOM Agent.

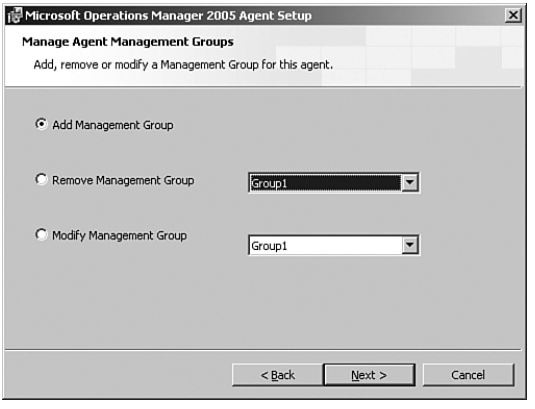


FIGURE 9.11 Addition, removal, or modification of management groups for the MOM agent.

5. The remaining steps are the same as with normal manual agent installation (discussed earlier in this chapter in the "Manual Agent Installation" section). These screens provide the configuration information for the management group, specify the MOM Agent Action account, and enable you to choose whether the management server is in a trusted Active Directory domain.
6. Continue to the Ready to Install page where you will verify your configuration and then start the installation.

Using Multihomed Agents

Organizations that have multiple physical locations often use multiple management groups. This strategy enables MOM 2005 to provide an effective monitoring environment

on a per-location basis and to roll up alerts to higher-level MOM servers. Figure 9.12 illustrates multiple management groups and a multihomed server configuration.

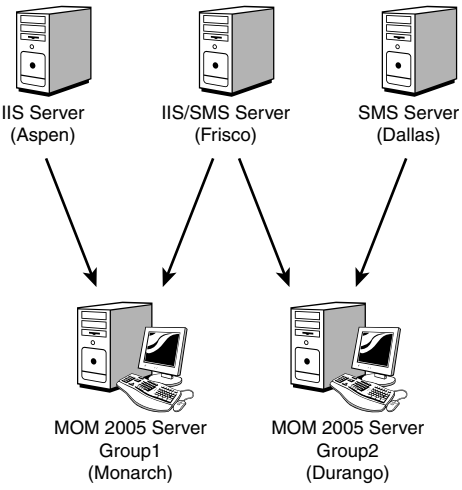


FIGURE 9.12 Multihomed SMS server (Frisco) in two management groups.

Multihomed architectures are also typically used in testing environments, for upgrade deployments, with security monitoring, or to separate performance data collection to decrease alert latency in high-volume environments. Multihoming can even be used as a migration technique as discussed in Chapter 7, "Upgrading to MOM 2005."

Real World—Using Multihomed Agents

Generally, the best architectural design for large-scale MOM setups is to avoid multihomed agents and instead to consider a multitiered architecture that provides at least two management servers per management group. This is discussed in more detail in Chapter 10, "Complex and High Performance Configurations." An exception to this rule is when you use a multihomed agent configuration to split out security log information.

Integrating Agentless-Managed Systems into MOM 2005

Agentless-managed systems can integrate into the MOM 2005 environment with most of the functionality available to full agent-managed systems. Items that agentless-managed systems support include state monitoring, service discovery, performance collection, internal service monitoring events, script execution, heartbeat, and event collection. Agentless configurations are best used in situations where an agent either cannot be deployed onto the system or cannot be deployed until a specific window of time (examples include scheduled outages or change control windows).

Limitations of agentless monitoring include the following:

- Some management packs do not support agentless management. If you need specific management packs to gather information from your agentless systems, test the management pack in an agentless configuration to determine whether it functions correctly. For example, the Active Directory Management Pack requires installed agents on all domain controllers.
- Because the event log information is gathered from the agentless machine and is displayed on the management server, the event log entries are not correctly displayed unless the management server has the same EventLogMessages.dll as the agentless computer.

Generating Event Log Entries

If event log entries for a particular software package are not being generated correctly on the MOM server, a potential workaround is to install the software package on the management server itself. This enables MOM to display the event log entries effectively for the software package.

- To function, agentless management requires remote procedure calls (RPC) and Distributed Component Object Model (DCOM) communication. In MOM 2000, the Agent Manager uses RPC for communication between the agent and the Data Access Server Consolidator Agent Manager (DCAM). In MOM 2005, RPC communication is used for agentless monitoring and for installing agents but is not required for MOM 2005 agents to function after installation.
- The Management Server Action account must have the same level of privileges that a local action account requires on the system being managed in an agentless configuration.
- Agentless monitoring does not support application log providers. The application log provider enables a management pack rule to use text log file data for monitoring. The provider is extensible, which enables management pack authors to use virtually any text log file meeting the requirement that each entry in the log file is stored on a single line of text.
- MOM 2005 supports a maximum of 10 agentless computers per management server, and a maximum of 60 agentless computers per management group.
- Agentless monitoring requires consistent network communication between the agentless computer and the management server. If network communication is interrupted, data can be lost.
- Additional network traffic is generated by using agentless monitoring as compared to traffic from computers with an installed agent.

Deploying Agentless Monitoring

Agentless monitoring can be deployed to systems that are located in the Unmanaged Computers folder. This folder is available in the MOM 2005 Administrator console, under Administration \ Computers \ Unmanaged Computers.

To deploy agentless monitoring, complete the following steps:

1. In the Detail pane of the Unmanaged Computers folder, right-click the system on which you want to monitor (or select multiple systems to deploy agentless monitoring on all at the same time), and choose Start Agentless Management from the context menu.
2. Click Yes when you receive the message Are You Sure You Want To Start Remotely Managing The Selected Computers Using The MOM Management Server?
3. Refresh the Unmanaged Computers folder. The specified system should disappear from this view.
4. In the Navigation pane, click Agentless-Managed Computers, and you should now see the system in the list.

Changing Agentless Managed to Agent Managed

Systems that are currently agentless monitored cannot be changed directly to agent managed because you must first deactivate agentless management. To initiate this task, complete the following steps:

1. In the Administrator console, open the Agentless-Managed Computers folder under Administration \ Computers \ Agentless-Managed Computers.
2. In the Detail pane, select one or more systems on which you want to install an agent.
3. Right-click and choose Stop Agentless Management from the context menu.
4. Click Yes when you receive the message Are You Sure You Want To Stop Remotely Managing The Selected Computers Using The MOM Management Server?
5. Refresh the view of the Agentless-Managed Computers folder, and the selected system no longer appears in the list.
6. In the Navigation pane, click Unmanaged Computers, and you will see the computer in the Unmanaged Computers list.
7. To install an agent on the system, follow the process in the “Deploying Agents Using the Administrator Console” section earlier in this chapter.

Identifying Unmanaged Computers

The Unmanaged Computers folder displays a list of systems discovered using the computer discovery rules that do not currently have an agent installed or agentless monitoring configured. Although not all options are necessarily populated, the following options are displayed for unmanaged computers: Name, Domain, Description, Operating System, Time Added, and Management Server.

The Unmanaged Computers folder is most often used to identify computers without agents installed or to install agents on unmanaged computers. Figure 9.13 shows an example of the Unmanaged Computers folder.

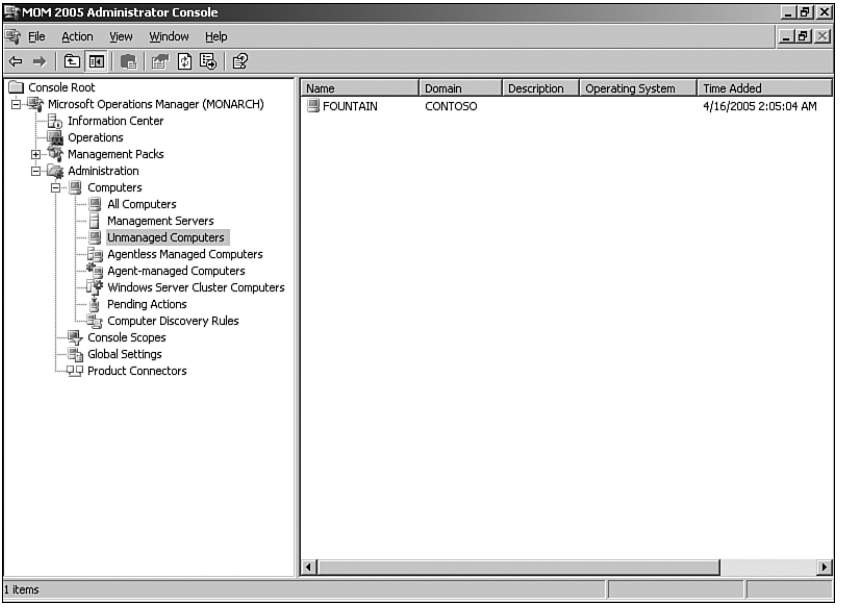


FIGURE 9.13 Unmanaged Computers folder.

Removing a Computer from the Unmanaged Computers Folder

If you no longer want to see a computer in the Unmanaged Computers view, remove the discovery rule that discovers the agent, create an exclusion rule to prevent the system from being rediscovered, and then delete that computer entry in the Unmanaged Computers folder.

Managing Agents

A number of tasks are associated with managing the agents in your environment. This section describes the concepts of pending actions, how to migrate and rename agents and computers that have the MOM agent installed, and how to remove agents.

Pending Actions

By default, the global setting for all management servers does not automatically install, uninstall, or upgrade agents as a result of computer discovery. This enables the MOM administrator to choose which installations occur rather than have agents automatically deployed. As MOM discovers new systems for installation, uninstallation, or upgrade, it places them in the Pending Actions folder until you have approved them.

MOM Agent Deployment

When you deploy MOM 2005, you may decide to keep the default setting to not automatically install, uninstall, or upgrade agents. This setting enables you to set discovery rules that will discover all servers in your environment and then phase in the specific servers on which you want to install the MOM agent. If you use automatic management, you need to strictly control which systems are discovered to avoid autoinstallation of the MOM agent on servers you might not want monitored.

The Automatic Management setting can be changed either for a single management server or globally for all management servers:

- For a single management server—Under Administration \ Computers \ Management Servers, right-click the management server for which you want to change the configuration; then choose Properties from the context menu. Clear the Use Global Settings option to configure the management server, and then click the Automatic Management tab and choose the Automatically Install, Uninstall, and Upgrade Agents and Automatically Start and Stop Agentless Management option.
- For all management servers—In the Administrator console, choose Administration \ Global Settings. Right-click Management Servers and choose Properties. Click the Automatic Management tab and choose the Automatically Install, Uninstall, and Upgrade Agents and Automatically Start and Stop Agentless Management option as shown in Figure 9.14.

Agent Settings

The default configuration is that agents communicate with the management server through port 1270 using both TCP and UDP. If an agent is installed manually and the control level is set to Full, additional ports are used during the setup process and during the agent scan process.

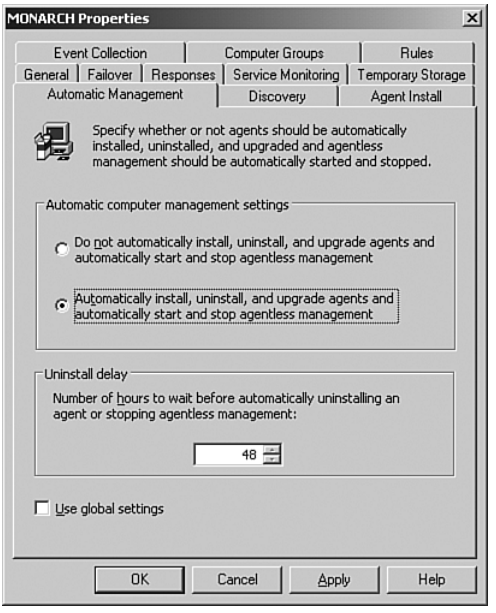


FIGURE 9.14 Automating computer management settings.

To change the default port number, complete the following steps:

1. In the Administrator console, click Administration, Global Settings.
2. In the Details pane, right-click Communications and select Properties.
3. In the Communications tab, change the communication port to the new port number, and restart the MOM service on the management server. Changing the port number has the following consequences:
   - Any manually installed agents will need to have the manual agent setup program rerun to point to the new port number.
   - Any agents that were installed by using the MOM 2005 Administrator console will begin communicating through the new port number after they receive the updated configuration settings; no additional configuration steps are required.

You should verify on your routing and firewall equipment that communication from the systems with agents to the MOM servers is allowed through the newly specified port. To determine whether communication is allowed between the servers using the new port number, complete the following steps:

1. Log on to the server with the MOM agent installed.
2. Click Start, Run, and type **cmd** in the Open box.

3. From the command prompt you can telnet to the management server on the port number to determine whether communication is allowed. For example: `telnet Monarch 1270`.

   If the screen goes blank with a blinking cursor, the connection is functional. If you receive a message that it could not open the connection on the host, there is a communications issue between the two systems or the service is not accepting connections on that port number.

Port Query Utility

Microsoft provides a GUI utility to test communication to TCP or UDP ports. It is available at http://download.microsoft.com when you search for PortQry Version 2.0.

Changing Agent Configurations

When the agent is installed on a system it can be assigned to one or more management servers and can be part of one or more management groups. The managed computer often is a member of a domain. Specific processes are required to change the configuration, domain membership, or computer name of an agent; these processes are discussed in the following sections.

Migrating Agents to Another Management Server

In some situations, you might decide to migrate agents from a current management server to a different management server. For example, if one management server is overutilized and another management server is underutilized, you can migrate agents to redistribute the workload.

You can configure an agent to report to a different management server by changing the computer discovery rules for the system. To reconfigure the agent, complete the following steps:

1. In the Administrator console, select Administration \ Computers \ Computer Discovery Rules.
2. Right-click the discovery rule that applies to the agent being configured, and select Properties from the context menu.
3. In the Management Server box select a new primary management server, and click OK.
4. Right-click Computer Discovery Rules, and click Run Computer Discovery Now.
5. To verify that the agent is reporting to the new management server, click Agent-Managed Computers, find the target agent computer, and then check the Management Server column to determine the primary management server for the computer.

6. To send the configuration change to the agent computer, right-click the target agent computer and click Update Agent Settings.

Migrating Agents to a New Management Group

The following are two methods to migrate an agent to a new management group:

- Uninstall the agent from the first management group, and reinstall the agent in the new management group. This option is best when your environment permits monitoring to be interrupted during the migration process.
- Migrate the agent by multihoming the agent/installing it into the new management group. Use this option if you cannot interrupt the monitoring during the migration process. When monitoring from the new management group is successful, uninstall the agent from the original management group.

Moving an Agent Computer to Another Domain or Renaming the Computer

To move an agent-managed computer from one domain to another you must first uninstall the MOM agent. After moving the computer, reinstall the agent. Any data in that was in the OnePoint operational database in the original domain is deleted when the agent is deleted from the Unmanaged Computers view.

Removing Agent Removes Data from MOM

Any time a computer is completely removed from MOM (not just moved to Unmanaged, but actually deleted from Unmanaged), operational data associated with that system is also deleted. Data already transferred to the MOM Reporting database (SystemCenter Reporting) will be accessible as historical data.

When installing a managed system in a different domain, you should also delete all discovery rules that are of rule type Include where Computer Name is the name of the computer with the agent being migrated from the original domain (if any), and re-create those rules in the target domain as necessary.

To rename a computer with an installed MOM agent, once again you uninstall the agent and delete all discovery rules that are of rule type Include where Computer Name is the computer with the agent being migrated (if any). Rename the computer and reinstall the agent.

Moved Machines Still Appear in the Operator Console

A machine that is simply renamed or moved to another domain without taking the preceding actions still appears in the MOM Operator console but will no longer report back to MOM.

Removing Agents

You have two options available to remove a MOM 2005 agent from a system. The recommended approach is to leverage the MOM 2005 Administrator console to uninstall the agent. In certain cases, you might be required to uninstall the client manually.

Removing Agents Using the Administrator Console

When using the MOM 2005 Administrator console to uninstall the agent, first remove the discovery rule targeting the server from which the agent will be removed. For example, if we want to remove the MOM agent for a server named Fountain, first remove the discovery rule(s) that discover Fountain.

To uninstall the agent select Administration \ Computers \ Agent-Managed Computers. Right-click the computer system to uninstall (in this case Fountain) and choose the Uninstall Agent option to launch the Uninstall Agents Wizard as shown in Figure 9.15. Specify a domain\username and password that has permissions to uninstall the agent. When the uninstallation is completed, the system is removed from the Agent-Managed Computers folder. The computer can then optionally be deleted from MOM by selecting Delete on the context menu of the computer in the Unmanaged Computers view.

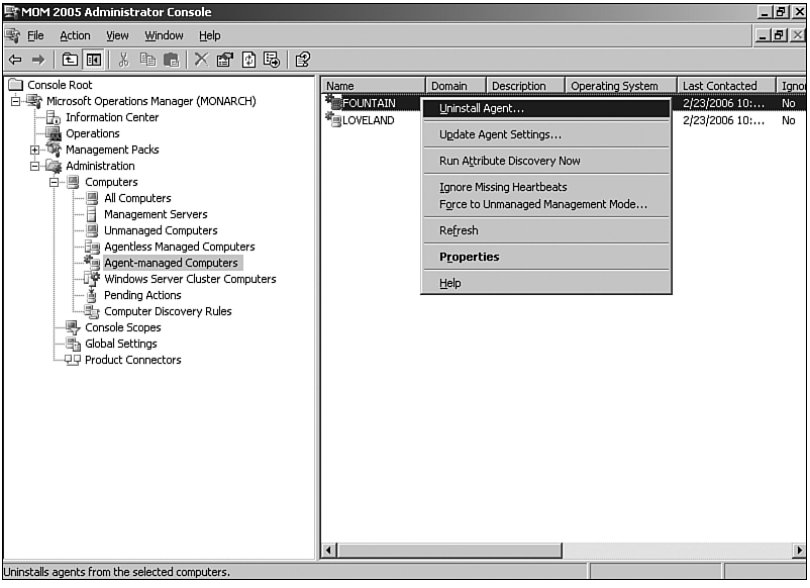


FIGURE 9.15 Removing an agent from the MOM Administrator console.

Removing Agents Manually

Whenever possible, use the MOM 2005 Administrator console to remove agents. If you need to uninstall a MOM agent manually, first use the Administrator console to remove the discovery rule for the server from which the agent will be removed. This prevents MOM 2005 from rediscovering the system and trying to reinstall the agent.

To remove the agent manually, log on to the system running the MOM agent using Administrator credentials, and open Control Panel. In Add/Remove Programs, click the Microsoft Operations Manager 2005 agent, and then select Remove. The uninstall process removes the agent from the system.

The computer will go into the Unmanaged Computers view if there is network connectivity to the management server. The agent can then be deleted from the Unmanaged Computers view.

If the Agent cannot communicate with the management server during the uninstall or the computer hosting the agent is already gone from the network for whatever reason, use the Force to Unmanaged option in the Agent-Managed Computers view and then delete it from that view.

Manual Agent Removal

If the agent will not uninstall because of errors during the uninstallation process, the following procedure can remove it from the system. Go to the command line (select Start, Run, and type **cmd**) and type the following command where ***drive:*** is the location of the Momagent.msi file:

```
msiexec /I drive:\momagent.msi REMOVE=MOMXAgent /q
```

For example, if the Momagent.msi file is on the root of the C drive, the syntax is

```
msiexec /I c:\momagent.msi REMOVE=MOMXAgent /q
```

Troubleshooting Tips

Table 9.1 lists some of the potential errors that might occur when you work with agents in MOM 2005. The Knowledge Base Article Number can be used to get more detailed information in the Microsoft knowledge database at http://support.microsoft.com.

TABLE 9.1 Potential Processing Errors and Their Resolutions

Process Error	Error Message	Potential Cause	Knowledge Base Article Number or Resolution
Push installs, mutual authentication.	The MOM Server failed to perform specified operation on computer.	Several items do not function correctly when using MOM 2005 with a disjointed DNS namespace.	885739; fixed with MOM 2005 SP1.
MOM agent does not respond or send alerts.	Active Configuration Is Not Available error in the MOMService.mc8 file.	A registry subkey is missing under HKEY_LOCAL_MACHINE\SOFTWARE\Mission Critical Software\ONEPOINT\Configurations*ConfigurationName*\Operations\Agent.	892683; workaround provided in the article.

TABLE 9.1 Continued

Process Error	Error Message	Potential Cause	Knowledge Base Article Number or Resolution
Push installs.	Error code 5: Access Is Denied When Installing An Agent.	Windows Server 2003 SP1, hotfix available on the Microsoft website as part of the KB article.	895195; fixed with Windows Server 2003 SP1.
MOM agent application log.	MOM 2005 agent logs the Existing Connection Was Forcibly Closed By The Remote Host event.	If an agent does not respond within 1 second, the management server closes the connection to the agent. The hotfix is available on the Microsoft website as part of the KB article.	885416; fixed with MOM 2005 SP1.
The script AD Replication Monitoring.	Encountered a runtime error. Failed to determine whether the Windows Management Instrumentation (WMI) replication provider is installed. The error returned is Invalid Parameter.	The Replprov.dll file tries to access a pointer that is not valid. The hotfix is available on the Microsoft website as part of the KB article.	889054; fixed with Windows Server 2003 SP1.
Accessing the Administrator console.	Administrator console fails with The Remote Procedure Call Failed error message.	Application error: Faulting application dllhost.exe and faulting module ntdll.dll. The hotfix is available on the Microsoft website as part of the KB article.	896989; fixed with Windows Server 2003 SP1.
Error upgrading MOM Server or agent.	Error message in the *MachineName* AgentInstall.log file or in the MOM*Component*.log file.	A previous installation of agent (MOM 2000 or MOM 2005) left behind registry keys from a previous agent installation.	888833; fixed with MOM 2005 SP1.

TABLE 9.1 Continued

Process Error	Error Message	Potential Cause	Knowledge Base Article Number or Resolution
Agent does not install on systems running Windows Server 2003 SP1.	Computer Management Task Summary: 1 Agent Install(s) Failed, Error Code: <;$MI>2147023174, Error Description: The RPC Server Is Unavailable.	If Windows Firewall is running on the MOM server, agents cannot communicate with the MOM server. If Windows Firewall is running on a destination computer or potential MOM agent, the MOM server cannot perform a push installation of the agent.	885726; workaround provided in the article.
Agent functionality.	Various agent installation and reporting errors.	Some products, including EMC Control Center and the NetIQ Security Manager, can cause conflicts with the MOM 2005 agent.	Fixed in later releases of both products.
Agents cannot communicate with the MOM server.	Various agent installation and reporting errors.	Mutual authentication is enabled in scenarios where mutual authentication will not function correctly.	Refer to Chapter 11 for technical details on mutual authentication.
Cannot perform various tasks on agents.	Errors during installation, uninstall, updating and upgrading agents.	MOM 2005 SP1 on the same server with Exchange and the MOM action account is running as Local System.	923107.
Agents not appearing in the Operator console.	No errors displayed, but no agent appears in the Operator console and alert or event information is received from them.	In environments with a large number of management packs installed the amount of configuration data may be larger than 1MB.	921988; a hotfix is available for this issue.

Summary

This chapter provides an understanding of the types of monitoring available within MOM (agent-based and agentless) and how MOM identifies systems for integration with MOM 2005. In the next chapter, we will discuss MOM implementations using complex and high-performance configurations.

CHAPTER 10

Complex and High Performance Configurations

IN THIS CHAPTER

MOM 2005 can provide solutions running on a single server, or it can scale to multiple servers depending on the specific needs of your organization. This chapter offers insight for deploying MOM 2005 in high performance environments requiring redundancy, multihoming, or multitiered configurations under various management server configurations.

Management Server Configurations

Many management server configurations incorporate a "complex" MOM environment. These include multilocation deployments, multitiered deployments, multihomed deployments, and redundant configurations (which we will discuss in the "Redundant Configurations" section of this chapter).

Multilocation Deployments

Our fictitious company Contoso's campus includes a corporate Dallas location (supporting 500 servers with the load split between two management servers named Monarch and Keystone). Contoso recently purchased a second company that has 100 servers in Houston.

Multiple Management Servers for Load Balancing and Redundancy

A common practice is to have at least two management servers in your primary location (which typically is where the database server resides), and split the agents between the management servers to provide load balancing and redundancy when a management server is not available.

Contoso installed a wide area network (WAN) link between the Dallas and Houston locations and is placing an additional management server in Houston as shown in Figure 10.1. The management server in Houston communicates with the database server in Dallas. A local management server keeps each agent in Houston from needing to communicate with a server in Dallas, which reduces bandwidth requirements.

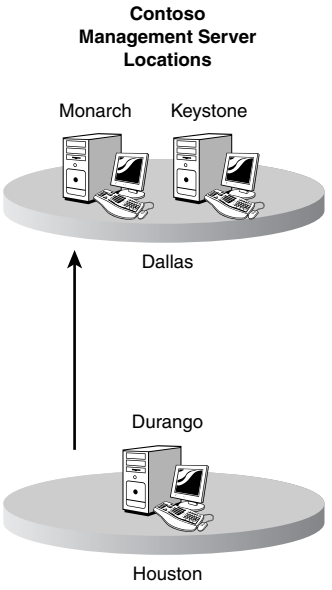


FIGURE 10.1 Management Servers in Dallas and Houston.

Although this example can also be architected as a multitiered configuration, Contoso decided to keep a single management group with a centralized database and use multiple management servers to localize its server management. A potential downside of this configuration is that one of the management servers (Durango) is accessing the MOM database across a WAN link. You would want to allow for this additional traffic when analyzing your WAN requirements. Microsoft recommends that if possible you use high-bandwidth communication links between the management server and MOM database, MOM database and MOM reporting server, and the management server and Administrator and Operator consoles.

Real World—How Much Traffic Is Generated?

Any time you mention traffic, the question always is "How much?" The answer really is "it depends." The amount of traffic here is contingent on the amount of database access across the WAN to the database server—which depends on the number of agents, number of management packs, and amount of activity being generated. The amount of traffic is also affected by the use of the various MOM consoles on the WAN segment.

In our own testing we have seen that a single agent reporting to the MOM management server creates at least 165Bps (.16Kbps) of traffic between the MOM management server and the MOM database server when only using the MOM 2005 management pack. The traffic increases to at least 452Bps (.45Kbps) of traffic when the Active Directory, DNS, and Base Operating System management packs are added (this being more than a 250% increase in traffic caused by adding a just a few management packs). These statistics represent stable systems only reporting back heartbeat and performance metric information. Actual network utilization on a per-agent basis should be higher than the statistics we are discussing here.

This leads us to a formula for estimating the minimum bandwidth requirements at # Agents * .45Kbps.

At this rate of traffic, the network connection between a database server connected to the management server via a 128Kbps link would be 80% utilized if there were approximately 226 agents reporting to the management server.

This number represents minimum network utilization between the management server and the MOM database. As the amount of information being sent from the agent increases, the network utilization will also increase.

Multitiered Deployments

In addition to implementing multiple management servers, you can deploy multiple management groups. As discussed in Chapter 4, "Planning Your MOM Deployment," multiple management groups should be used in situations such as:

- Exceeding management group support limits (more than 4,000 computers in a management group)
- Exceeding management group support limits for agentless systems (more than 60 in a management group)
- Separating administrative control (operating systems managed by one support group, applications by another group)
- Splitting geographic locations (multiple locations with servers at each location)
- Network environment restrictions (minimal bandwidth or reduced network traffic requirements)

Capacity Planning for Multiple Management Groups

If you create a second MOM management group, you must decide how best to separate the agents across the two management groups. Common approaches include splitting the agents geographically, or by departments. For example, one IT department may have control over its group of servers but no control over a second IT department's servers.

Allow for growth in the number of agents within your management groups and do not attempt to configure more than 4,000 agents (the maximum supported) in a single management group. As part of your planning process, consider connecting the two management groups using the MOM Connector Framework (MCF) and the MOM-to-MOM Product Connector (MMPC). These tools are discussed in Chapter 19, "Interoperability."

Establish a Central Management Group and Consolidated Operator Console

Multiple management groups can be structured in a hierarchy, and you can use the MCF and MMPC to forward alerts and client discovery data to a central management group. A hierarchy enables you to implement an enterprisewide MOM Operator console, providing a view of your entire organization and a single location for managing alerts. For example, Figure 10.2 shows a three-tiered management server implementation for a North American corporation (Contoso), with server operations in Texas and Illinois. This is a three-tiered management server implementation because Dallas reports to Texas which in turn reports to North America.

With this configuration Contoso utilizes a North America operations support staff along with a Texas regional support staff, where alerts can be managed at both levels. MOM forwards alerts from one management group to a higher-tiered management group with the MOM Connector Framework and MOM-to-MOM Product Connector.

Multitier Alert Forwarding

In a multitiered configuration, each alert in the subordinate MOM group that needs to be forwarded to the parent MOM group must be selected and its properties modified to configure the rule to be forwarded. As a result, selecting this subset of alerts is critical and can be a time-consuming process.

Another potential issue with multitiered environments is that the MOM management packs must be synchronized across the tiers. A process for exporting and importing MOM management packs should be created and documented to maintain a multitiered configuration.

Multihomed Deployments

As discussed in Chapter 5, "Planning Complex Configurations," a multihomed configuration exists when the agent on a server reports to more than one management group. Each management group has its own OnePoint database and management server(s). (An agent reporting to multiple management servers within a single management group is *not* multihomed.)

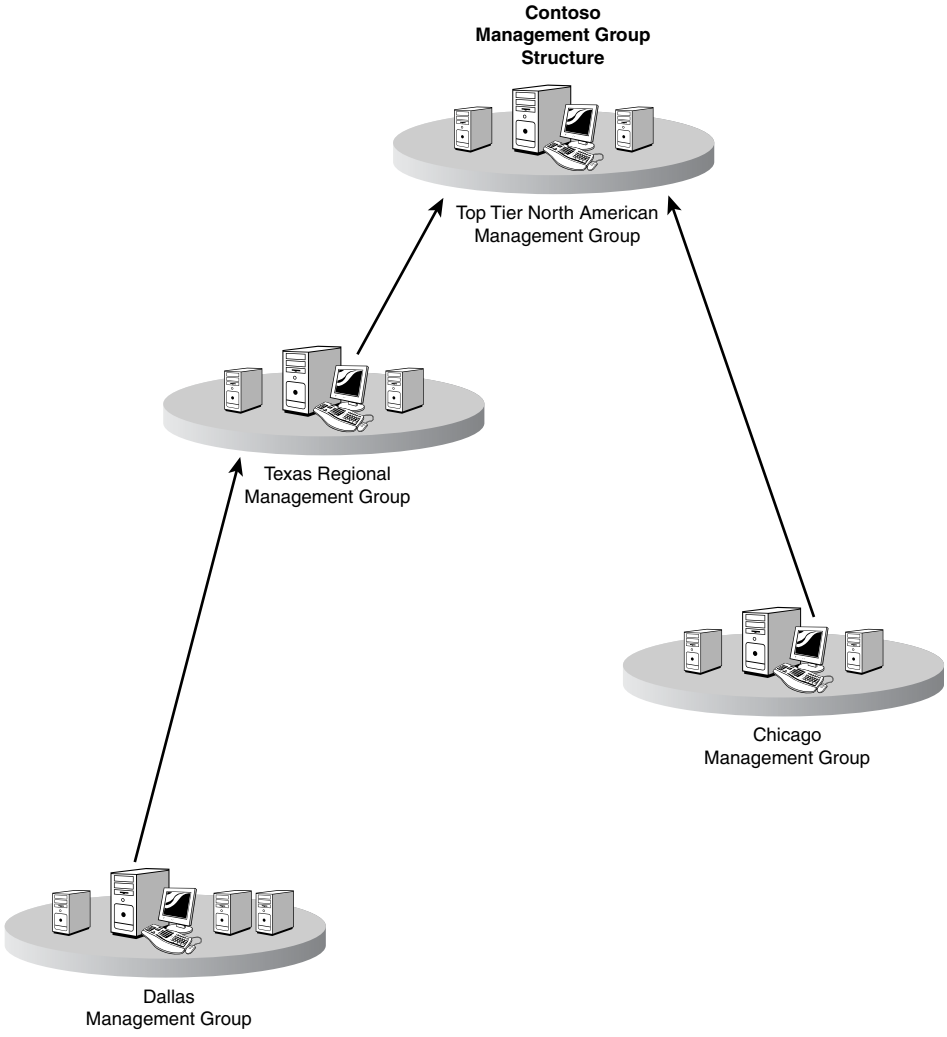


FIGURE 10.2 A three-tiered management server implementation.

Multihoming allows you to distribute monitoring across multiple technical teams. For example, your security administrators can monitor a computer for security issues, while your Exchange administrators monitor the same system because it runs Microsoft Exchange. By installing multiple management groups and then multihoming agents, you can distribute monitoring requirements across multiple teams—enabling each team to use separate MOM administrators and rule configurations. Because each management group has its own database, you can change rules in one group without impacting rules in another management group.

A multihomed agent can report to a maximum of four management groups. Each management group has its own set of processing rules and configuration information. A multihomed agent processes each set of processing rules independently, so there is no conflict of rules. The agent can use a different Action account for each management group—which allows management group administrators to determine their own Action account security requirements.

Multihomed agents can be deployed using the same mechanisms discussed in Chapter 9, "Installing and Configuring Agents." The agent can be installed using the Add Computer Wizard in the Administrator console or by manual agent installation. To install a multihomed agent just install the agent in one management group and then install it in the second management group.

Figure 10.3 shows a sample multihomed configuration with two management groups (Group1 and Group2) reporting to two different management servers (Monarch and Durango).

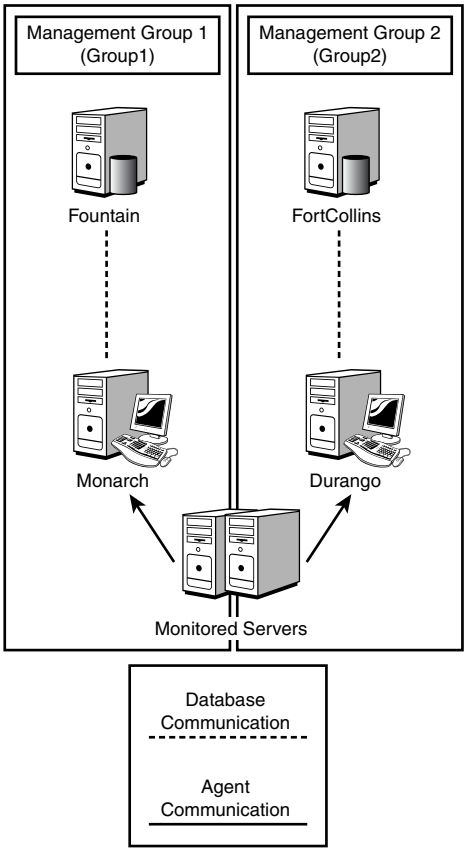


FIGURE 10.3 A sample multihomed configuration.

As you can see, there are a variety of ways to implement management servers and management groups. Evaluate these options and consider the best course of action based on your specific business requirements.

Redundant Configurations

As discussed in Chapter 4, although all MOM components can be configured on a single server, for performance or high availability reasons you may decide to use a multiserver implementation. A high level of uptime is best achieved using redundant MOM configurations, which require a multiserver implementation.

Order of Installation for Redundant Configurations

Installing a redundant MOM configuration requires identifying the necessary steps and the order in which they will occur. The following steps provide the recommended order for installing redundant configurations. Later sections of this chapter go through specific procedures as indicated:

1. Install and patch the operating systems on all MOM servers (management, database, and reporting).
2. Configure and test load balancing for any servers requiring network load balancing capabilities, which typically is the web servers used with MOM Reporting.
3. Configure and test clustering on any database servers indicated—the MOM OnePoint database and/or MOM Reporting database.
4. Install and patch SQL Server on the database server(s).
5. Install and patch SQL Reporting Services on the reporting server.
6. Install the MOM database server(s) for your clustered configuration. This is covered in the "Database Servers" section later in this chapter.
7. Install the MOM management server(s), discussed in the "Management Servers" section later in the chapter.

Managing Failover Using Multiple Management Servers

When two management servers are available in the same management group, failover occurs when the primary server is unavailable. When more than two management servers are available in the same management group you can specify which management server will provide failover for the other management servers. For example, if we have three management servers (Monarch, Keystone, and Durango) we can configure Durango to be the failover for Monarch but not allow Keystone to be the failover server for Monarch. Failover configuration is maintained in the Administrator console under Administration \ Computers \ Management Servers, by right-clicking on the management server, and choosing the failover tab.

If you install more than two management servers into a management group and want to configure specific agents to fail over to specific management servers, this can be

configured when manually installing the agents. On the Advanced tab of the agent configuration screen you can specify the alternate management server for a specific agent. For details on the process to manually install agents see Chapter 9.

8. Install the MOM reporting server(s) as described in the "Reporting Servers" section later in this chapter.
9. Install the MOM reporting database server(s). The appropriate steps are specified in the "Reporting Database Servers" section later in this chapter.

Management Servers

As discussed in Chapter 5, installing multiple management servers in the same management group provides redundancy in case management servers go down. If an agent's primary management server is unavailable, it sends its data to what is known as a *failover management server*. The agent continuously retries contacting its primary management server; when it reestablishes communication with its primary server, it sends data to that server.

MOM 2005 supports a maximum of 10 management servers in a single management group. Determining the optimal number of management servers depends on several factors, including the number of computers being managed and the geographical locations of those computers.

Implementing Database High Availability

For a high-availability environment you may also want to consider clustering the MOM database. We discuss clustered implementations for the OnePoint database in the "Database Servers" section later in this chapter.

Installing Multiple Management Servers in a Management Group

The process is straightforward for installing additional management servers. You run the MOM 2005 setup process on the target server but only select the components associated with the management server itself. Initially, our example environment had a single management server installed for the management group (Monarch). To provide redundancy for the management servers we installed an additional management server, Keystone. The following steps install Keystone as an additional management server:

1. Verify that the server meets the hardware and software prerequisites outlined in Chapter 6, "Installing MOM 2005."
2. Run MOM setup (setup.exe) from the MOM 2005 installation media. At the Welcome screen, select the option to install MOM, which is the second item on the Setup Tasks tab. After confirming the license agreement and product registration key, you are asked to specify a setup type on the installation options panel. Be sure to select Custom.

3. At the Custom Setup screen, specify the components to install. Make sure that you uncheck the MOM 2005 Database component! You can install the MOM Administrator and MOM Operator consoles by leaving the MOM 2005 User Interfaces selected. Figure 10.4 shows the correctly selected components for installation.

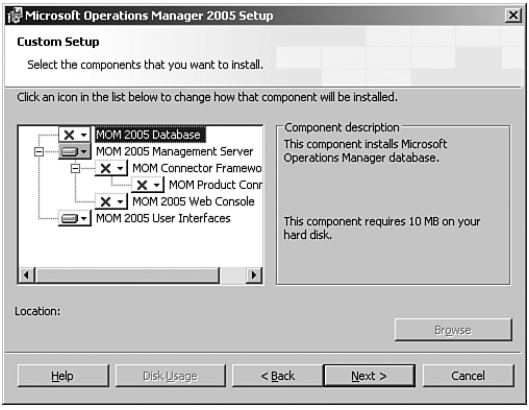


FIGURE 10.4 The Custom Setup components screen to install an additional management server.

4. The Check Prerequisites utility automatically runs as part of the installation process. Correct any errors and check any warnings generated by the Prerequisite Checker.
5. You are next asked to specify the MOM 2005 database server name and SQL Server port. Enter the values for your existing MOM 2005 database server and SQL Server port. (By default, the SQL Server port is 1433.)
6. You are prompted for the Management Server Action account. The Action account installs MOM agents and runs responses on behalf of agents. This account needs appropriate permissions in the domain in which you are installing the management server. Specific rights required by the Management Server Action account are discussed in Chapter 11, "Securing MOM."
7. You are now asked to indicate the Data Access Service (DAS) account. The DAS account must have appropriate rights in the OnePoint database. Use the DAS account that your other management server(s) use.
8. After the DAS account is specified, Setup runs the installation process.

After a successful installation, you can configure the new management server for use. Create new discovery rules for the agents you want to monitor with this server. There are some potential issues in defining discovery rules when you have multiple management servers, which we will discuss in the next section.

Defining Discovery Rules

When you use multiple management servers, take care to create discovery rules specific to each management server. Do not overlap these discovery rules or you will have systems managed by both management servers. Using wild cards (*) in your discovery rules can cause unintended overlaps between the management servers, so be careful when defining rules that use wild cards. If you use the ManualMC.txt (a text file including server names for discovery) to list the agents on each management server, make sure that you do not have overlapping entries there either.

Using the ManualMC.txt File

Chapter 9, "Installing and Configuring Agents," describes configuring the ManualMC.txt to discover agents.

Should your discovery rules (or ManualMC.txt entries) overlap between management servers in the same management group, the last server running its discovery cycle becomes the agent's primary management server. Having overlapping discovery rules causes a managed computer to continuously change its primary management server. When the agent switches from one management server to another its heartbeat statistics are not reliable and rules using state variables do not function properly. The content of state variables (which can track things such as the number of times something has occurred) is reset if the agent changes its management server.

Tracking Agent Switching of Management Servers

Event 21056 is generated in the Application event log when an agent changes its primary management server to a new management server.

Database Servers

If you require high availability for MOM 2005, creating redundant management servers is the first step but not an entire solution. Management servers require a functioning SQL Server database, and a single MOM database server constitutes a single point of failure. You can provide redundancy for the MOM database by using Microsoft Cluster Server (MSCS). MSCS provides redundant server nodes, allowing an application to be accessed from a standby node if the active node fails. MSCS implementations can be Active/Active, where each node actively supports an application or Active/Passive. An Active/Passive configuration has an active node and one or more passive nodes on reserve in case there is an outage on the active node. As discussed in Chapter 5, the number of nodes supported within a cluster varies depending on the operating system.

MOM 2005 supports clustering the OnePoint database with an Active/Active or an Active/Passive cluster configuration. There are several major differences between these approaches:

- When the MOM database is installed on an Active/Active cluster, each node in the cluster can contain its own OnePoint database running on its own SQL Server instance—meaning that both nodes in an Active/Active cluster can house the OnePoint database for a different management group. For example, if we have two management groups (contoso_admin and contoso_security) we could install SQL Server using two instances, and install the OnePoint database for each management group onto the cluster, as shown in Figure 10.5.

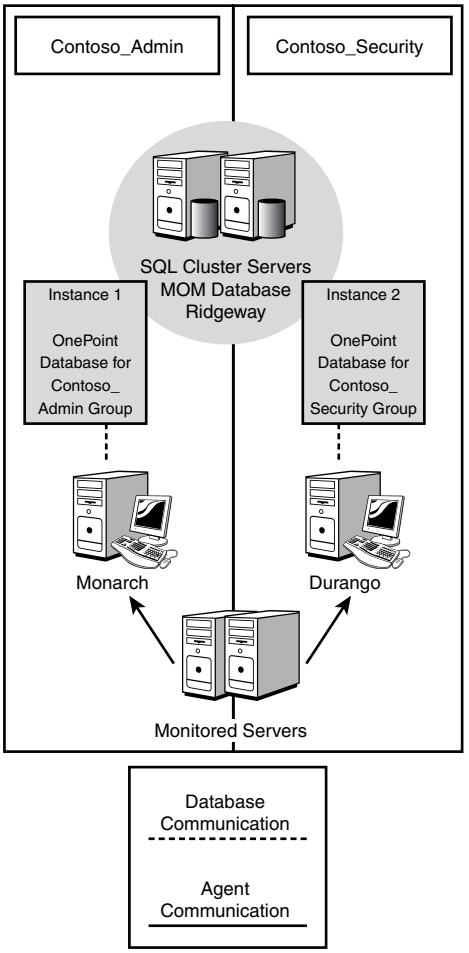


FIGURE 10.5 Active/Active SQL database cluster.

- With an Active/Passive cluster, the active node houses the OnePoint database; the passive node does not. MSCS moves the OnePoint database to the now active (formerly passive) node in the event of a failure.

Installing MOM in an Active/Passive or Active/Active cluster allows for redundancy and failover capability in the event of a failure of the active node. Clustering provides MOM 2005 with a high-availability database capability.

Installing MOM 2005 on an Active/Active SQL Cluster

Let's step through the process to install a clustered OnePoint database on an active node using an Active/Active configuration. We will point out the differences between a "Typical" installation as described in Chapter 6, and those steps that are cluster specific. Active/Active is supported only with MOM 2005 Service Pack 1 installed.

The major difference in installing an Active/Active solution versus an Active/Passive configuration is that you must manually create the database for an Active/Active configuration. The standalone tool used to create the MOM 2005 database is MOMCreatedb.exe, located in the \SupportTools\x86 and SupportTools\ia64 directories on the MOM installation media.

You can use this utility to create and initialize a MOM database for several configurations:

- A database cluster in Active/Active mode
- A MOM database on a 64-bit database server
- Multiple MOM databases on different SQL instances located on the same physical machine or Active/Passive cluster (such as when using a cluster to house the OnePoint database for two different management groups).

Checking Installation Prerequisites Before Running MOMCreatedb

Run the MOM 2005 Prerequisite Checker prior to running MOMCreatedb.exe on the active node. Run setup.exe from the MOM 2005 CD and select Check Prerequisites, choosing the option to check prerequisites for the MOM 2005 Database only. This verifies whether the active node meets the requirements for a MOM 2005 database server.

1. Run MOMCreatedb on the Active cluster node. Figure 10.6 shows the configuration screen for the utility:
   - The SQL Server Instance points to the virtual SQL node, which in this example is Evergreen, and the instance of SQL on that node (SQLCluster in Figure 10.6).
   - The database file and log locations must reside on a physical disk resource belonging to the Cluster Group where the SQL Server instance is installed.

Specifying the Database Files Location

If you do not specify a location that is part of the Cluster Group, the database installation will fail.

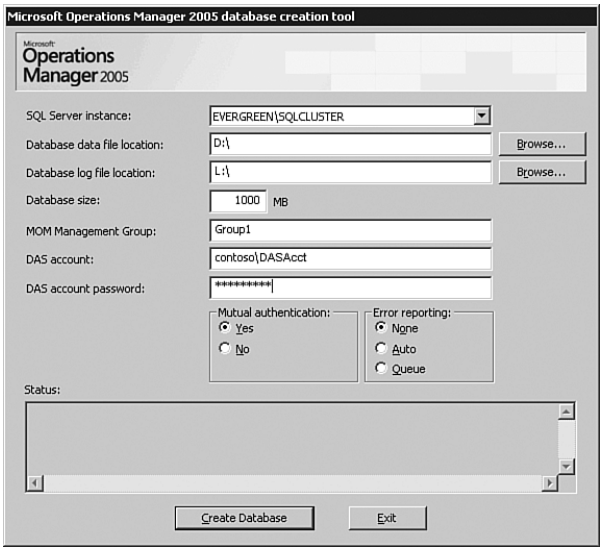


FIGURE 10.6 The MOMCreatedb.exe configuration screen.

- The other items on the configuration screen specify the database size, the MOM management group name (Group1), the DAS account and password, whether mutual authentication is enabled by default, and whether MOM error reporting is specified. Click Create Database to create and initialize the OnePoint database on the active node.

2. After MOMCreatedb.exe completes successfully, install your management servers by specifying the SQL Server instance in the MOM installation program, shown in Figure 10.7.

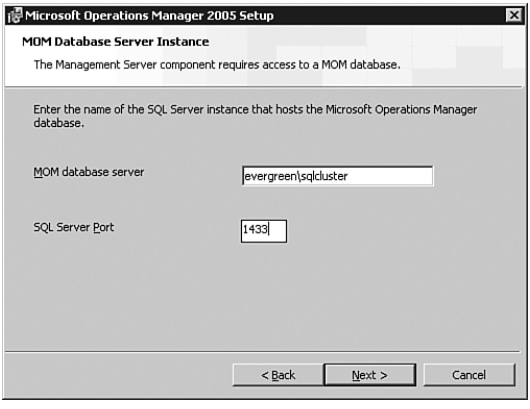


FIGURE 10.7 Specifying the SQL Server virtual instance.

We will now compare installing MOM with an Active/Active Cluster to the process of installing it with an Active/Passive SQL Cluster. Our example uses an Active/Passive cluster named Evergreen, but now one node is Active (Evergreen1), and the second node is Passive (Evergreen2).

Installing MOM 2005 on an Active/Passive SQL Cluster

To install MOM 2005 on an Active/Passive SQL Cluster, run the MOM installation program on each node in the cluster. It is not necessary to run MOMCreatedb.exe for an Active/Passive Cluster installation. The following procedure installs an Active/Passive Cluster in a MOM 2005 management group:

1. On the active node (Evergreen1), run setup.exe, specifying only the installation of the MOM 2005 database. Figure 10.8 shows the component screen with the MOM 2005 database selected.

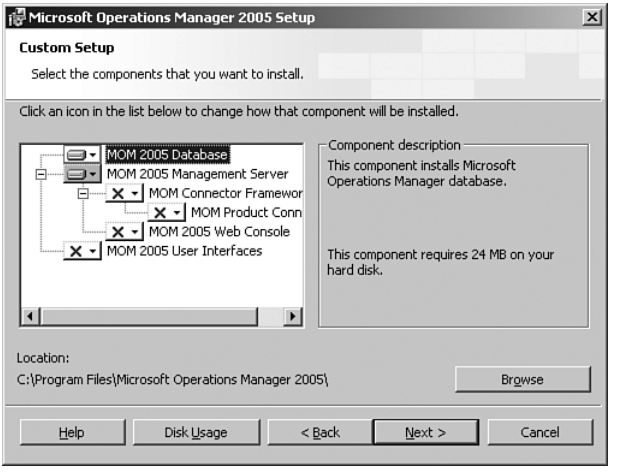


FIGURE 10.8 Configuring Setup for the database only.

2. Specify the location of the MOM database, which will be the virtual SQL Server Cluster node and instance. Figure 10.9 shows the screen configured with the virtual SQL Cluster node of Evergreen and the instance name SQLCluster.
3. At the Database and Log File Options screen, be sure that you specify a physical disk resource belonging to the Cluster Group where the SQL Server instance is installed. Figure 10.10 shows the data file location on the D: drive and the log file locations on the L: drive, both of which are physical disk resources in our Cluster Group.
4. After completing Setup for the OnePoint database on the active node, run Setup to install the database on each passive node in the SQL Cluster (Evergreen2). Figure 10.11 displays the difference from setting up the database on the active node—make sure that you select the Passive Node of a Windows Server Cluster check box.

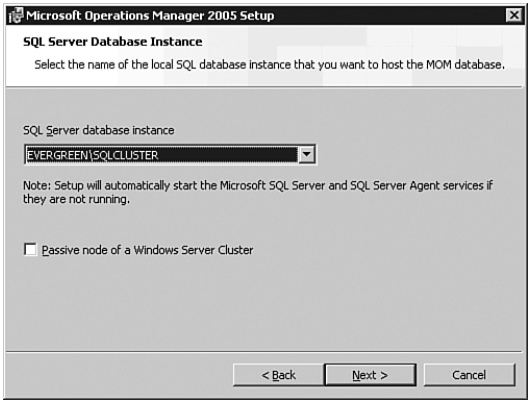


FIGURE 10.9 Specifying the Virtual SQL Server Cluster Node and Instance.

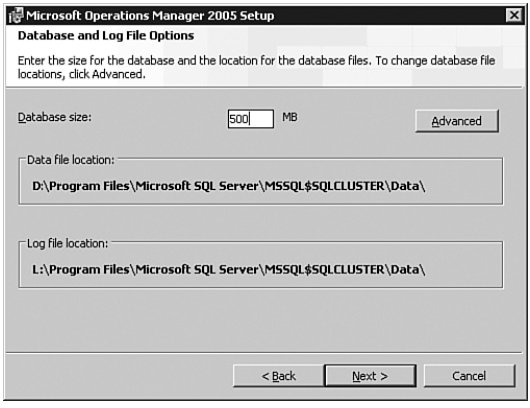


FIGURE 10.10 The database and log file options screen for the clustered database.

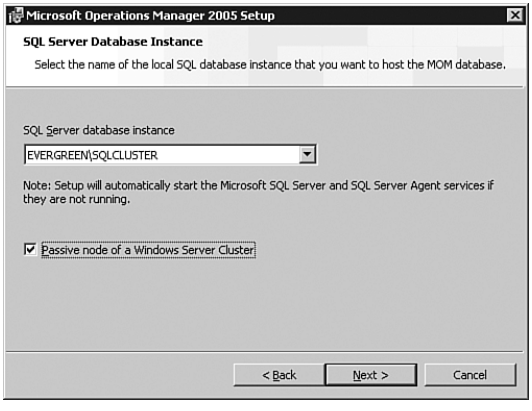


FIGURE 10.11 Configuring the SQL Clustered passive node for the OnePoint database.

Install MOM for Each Passive Node

Remember to run the setup installation program for each passive node in the Cluster. Installation of MOM on the passive node is required to properly configure registry keys. If MOM is not installed on the passive node the cluster will be unable to fail over to that passive node.

Real World—MOM Database Failover Processing

What takes place when the OnePoint database is installed on an Active/Passive Cluster and a failover occurs? From MOM's standpoint, nothing—the failover is transparent to MOM, although there is a slight delay in generating alerts during the failover until the SQL Server is online with the new Cluster node. The data is stored in MOM's queue files until SQL Server resumes communications with the DAS component and data can be inserted into the OnePoint database.

Appendix A, "MOM Internals," discusses MOM 2005 queue file processing.

Reporting Servers

High availability is typically not a requirement for the MOM 2005 reporting components, but there can be exceptions to that rule. As mentioned in Chapter 5, a more economical but less effective method to provide redundancy for the reporting database servers is using SQL replication to replicate data to another database. For most environments this provides an acceptable level of redundancy for the MOM reporting components. However, for the purposes of this example we are defining a high availability solution as 24x7x365 (24 hours a day, 7 days a week, and 365 days a year) uptime required. To provide this level of availability, MOM supports network load balanced Reporting servers and clustering the Reporting Database servers. For our example, we will install two Reporting servers (Breckenridge1 and Breckenridge2) using a Network Load Balancing (NLB) cluster name of Breckenridge. To install redundant reporting servers, you would perform the following steps:

1. Implement NLB on the servers that will provide reporting services.
2. Install and patch SQL Server on the reporting database server(s). Unlike the MOM OnePoint database, the Reporting database can only be installed on an Active/Passive cluster configuration. Active/Active configuration is not a supported configuration.
3. Install SQL Server Reporting Services (SSRS) Enterprise Edition on the first node of the NLB cluster (Breckenridge1).

SQL Server Reporting Services Enterprise Edition

Creating a SQL Server Reporting Services web farm requires the Enterprise Edition of SSRS. Standard Edition does not support redundancy using NLB.

4. Verify functionality by accessing the SQL Server Reporting Services website on the first node (Breckenridge1).
5. Install SQL Server Reporting Services on the second node of the NLB cluster (Breckenridge2).
6. Verify functionality by accessing the SQL Server Reporting Services website on the second node (Breckenridge2).
7. Apply the appropriate service pack level to SQL Server Reporting Services on the first node (Breckenridge1):
   - If you are running MOM 2005 SP1, apply SSRS SP2 to the first node.
   - If you are running MOM 2005 without a service pack, apply SSRS SP1 to the first node.

   Verify functionality by accessing the SQL Server Reporting Services website on the first node.
8. Apply the appropriate service pack level to SQL Server Reporting Services on the second node (Breckenridge2):
   - If you are running MOM 2005 SP1, apply SSRS SP2 to the second node.
   - If you are running on MOM 2005 without a service pack, apply SSRS SP1 to the second node.

   Verify functionality by accessing the SQL Server Reporting Services website on the second node.
9. Access the SQL Server Reporting Services website to verify that it is functioning on the NLB cluster.

   To validate the functionality of an NLB web cluster check the website from both the NLB cluster's name and from the individual server nodes within the NLB cluster. You should use a web browser on a system that is not a member of the NLB cluster and access the SQL Reporting Services website using the name of the NLB cluster. For example, the Breckenridge web NLB cluster would be accessed via the following Uniform Resource Locator (URL): http://breckenridge/reports. Check each of the individual nodes of the NLB cluster to validate that they are functional. For our examples these would be accessed as http://breckenridge1/reports and http://breckenridge2/reports.

Reporting Database Servers

Installing the reporting database on an Active/Passive Cluster is similar to the process of installing the OnePoint database on an Active/Passive Cluster. You install MOM Reporting on the active node and then install the passive node(s) in the Cluster. In this example the

reporting database cluster Ridgeway has two nodes, Ridgeway1 (Active) and Ridgeway2 (Passive). The following steps install MOM Reporting on the active node:

1. Run the MOM installation setup.exe program on the active node (Ridgeway1), selecting the option to Install Microsoft Operations Manager 2005 Reporting.
2. Specify the location of the OnePoint database and the SSRS server name. Specify the NLB's cluster name when asked for the location of the MOM Reporting database. If the installation will not continue when you specify the NLB cluster name, you can specify the name of the first node of the NLB cluster.
3. Specify the size of the reporting database and the location of the data file and log file. Be sure to use a physical drive resource from the Cluster Group to which the SQL Server Cluster belongs. Figure 10.12 shows this screen configured to create the data files on the D: drive and logs files on the L: drive, which are Cluster resources.

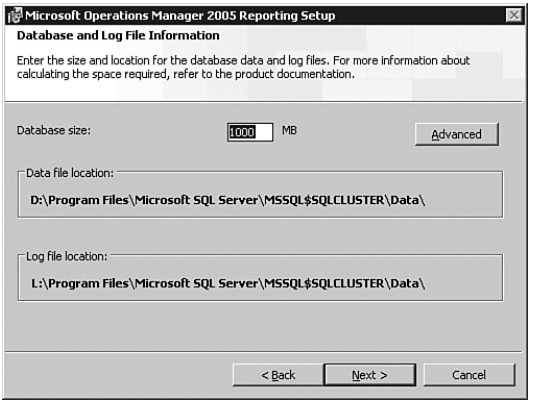


FIGURE 10.12 The Database and Log File Options screen.

4. The remaining screens in the setup process are the same as when installing MOM Reporting on a nonclustered server.

After installing the active node, install MOM Reporting on all passive nodes on the Cluster (Ridgeway2). Run setup.exe from the MOM 2005 installation media and select the option Install Microsoft Operations Manager 2005 Reporting. The difference in setting up the passive node is the SQL Server Database Instance screen as shown in Figure 10.13. You must check the passive node of a Windows Server Cluster check box.

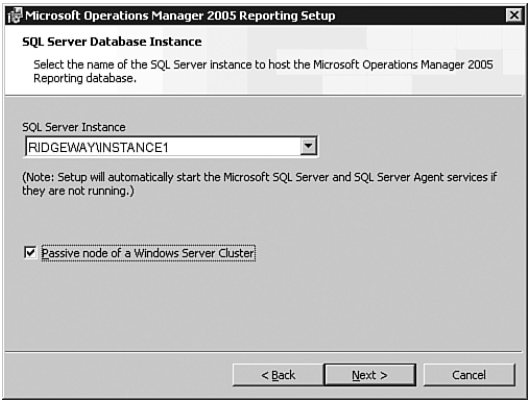


FIGURE 10.13 The SQL Server Database Instance Screen for MOM Reporting setup on a passive node.

After installing all passive nodes, perform the following configuration steps:

1. The DTS job is a scheduled task that runs at the operating system level (located under Control Panel, Scheduled Task) and needs to be configured to run only on the active node. Disable the Data Transformation Services (DTS) jobs on all passive nodes. Only one DTS job can be active for the MOM Reporting database.

   To disable the DTS jobs, on each passive node (for our example Ridgeway2) navigate to Control Panel / Scheduled Tasks / SystemCenterDTSPackageTask. Uncheck the Enabled check box and click OK to disable the DTS task on the passive node; be sure to do this for each passive node in the cluster.

   If there is a failover on the active node, you must manually reenable the DTS job on the system that is currently active, and disable the DTS job on the system now in passive node.

2. You will need to provide the appropriate access permissions to the MOM Reporting Components for the clustered MOM Reporting Database. On the active node on the cluster (Ridgeway1), use the Microsoft SQL Server Query Analyzer (or a SQL Server Management Studio query) to run the following SQL statements:

   ```
   Use SystemCenterReporting
   Execute p_SetupLogins '<machine name of the MOM Reporting Node>'
   ```

3. Verify that the two local MOM Reporting groups were created on the active node (Ridgeway1):

   - SC DW DTS
   - SC DW Reader

If these groups do not exist, they need to be manually created. The groups control who accesses the MOM reports and allow data to be transferred from the MOM database into the MOM Reporting database.

Information on Reporting Security Groups

More information on the SC DW DTS and SC DW Reader groups can be found in Chapter 11.

If any of the server names used for the redundant configuration discussion look familiar, they should! If you install each of the redundant systems as we have, your final results should look like Figure 10.14 as shown here. This configuration was also shown in Chapter 5.

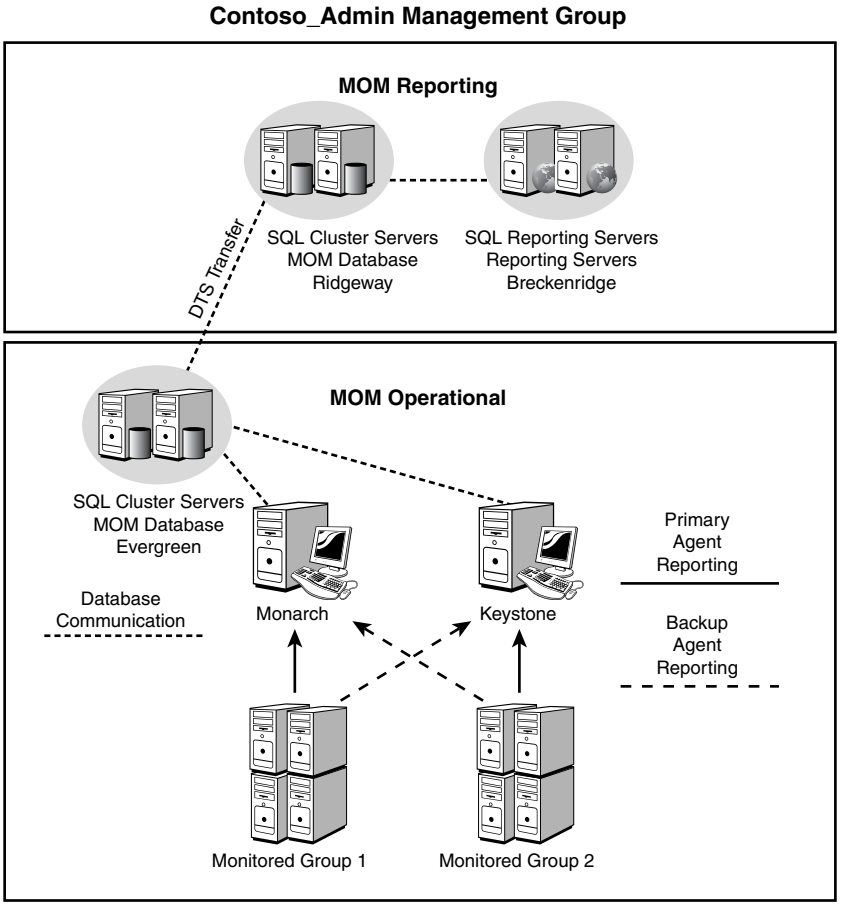


FIGURE 10.14 Fully redundant MOM configuration.

High Performance Configurations

MOM 2005 is designed to give prompt notification of issues and provides tools to help resolve those issues. Because we want to be notified of potential problems, we want MOM to operate efficiently and effectively. We can help achieve this by architecting MOM for performance, and avoiding and resolving bottlenecks.

Architecting for Performance

The first step in creating a high-performance MOM configuration is to design it from the beginning for performance. An inherently overloaded monitoring solution does not perform well. By following the concepts introduced in Part II, "Planning and Installation," particularly Chapter 4 and Chapter 5, you can understand the process for determining what is required in your environment and architect accordingly.

For example, you should be well aware of how many agents a management server can support. Using more than the supported number of agents can introduce overload situations for your management servers. This can be contrasted with the MOM reporting components, which typically are stressed only when generating reports and thus generally do not present significant performance issues.

Design your MOM environment to address any bottlenecks existing within the infrastructure. We discuss this in the "Avoiding and Resolving Bottlenecks" section later in this chapter. Your design should provide sufficient scalability to meet your business requirements. For management servers it is relatively simple to add management servers into a management group and then split the agents between the servers. However, the MOM databases can represent a more complicated architectural challenge. How do you architect MOM for performance if you don't include the database components as part of your strategy?

Using Chapter 4 as our starting point, we know that both your operational and reporting database server hardware should have at least a dual processor and one gigabyte of memory and may require up to a quad processor with two gigabytes of memory.

When architecting your database server use best-practice approaches for designing SQL Server to assist with providing a high-performance configuration. When possible put the SQL Server database on a dedicated server and add plenty of memory so that CPU and memory will not be bottlenecks. SQL Server can use additional memory effectively, so using the Enterprise Editions of Windows and SQL Server and adding memory beyond the 2 gigabytes recommended in Chapter 4 may provide additional performance benefits.

From a disk perspective, the more spindles it has the better the SQL Server performs. The preferred method is to configure your system using multiple drives for the operating system, SQL binaries and Windows page file, transaction logs, and data files:

- Use a Redundant Array of Independent Disks (RAID) 1 configuration for the operating system drive.

- Use RAID 1 or RAID 5 for SQL binaries and swap file because they are always read from.
- Use RAID 5 for the transaction log files.
- Use RAID 5 or RAID 10 for the database files.

The exception to this rule is when you are connecting your SQL Server to a Storage Area Network (SAN). In this situation you would use the following configuration:

- Use RAID 1 for the operating system drive (locally stored).
- Use RAID 1 or RAID 5 for SQL binaries and swap file because they are always read from (locally stored).
- Use the SAN to store the log files on one Logical Unit Number (LUN). The actual RAID configuration for the LUN is best determined by the personnel responsible for configuring the SAN.
- Use the SAN to store the database files on another LUN.

Another consideration for database performance is monitoring your database for growth. The size of the OnePoint database is dependant on the number of agents deployed, the number of management packs used, the stability of your environment (which impacts how much data is sent to the management server), and the amount of time data is retained in the database.

Controlling MOM Event and Alert Storms

Sometimes you need to capture many events with MOM and have an alert take some action. For example, one large organization was capturing group change events from the Security event log and sending an email to log them. This is not a problem for MOM; you just create an event rule to capture the events and an alert rule to send the email when the events are captured. Chapter 14, "Monitoring With MOM," discusses in detail how to create rules and alerts.

However, every so often, there could be many changes in group membership and then the email would not be sent. There would be an alert indicating that the rule had raised more than 50 alerts in 1 minute and that the rule had been disabled for 10 minutes. During that time, the emails that are supposed to log the group changes would not be generated.

This behavior is due to the MOM event storm protections. An event storm is a high volume of events that are logged in the MOM database and overload the MOM Administrator console. Event storms can be caused by a number of things, including, but not limited to the following:

- Hardware failures
- Network-related issues

- Security attacks or violations
- A particularly large number of events

MOM has built-in mechanisms to limit the amount of overload if a large number of events take place. For example, when a particular event ID occurs and matches the MOM consolidated rule defined for an agent, the rule will generate one alert within 60 seconds, instead of continuously generating an alert each time the rule engine finds a match.

Although this is normally a good feature to prevent the swamping of the console, in some cases the threshold of 50 alerts in a minute is too low. The registry keys in Table 10.1 allow you to control the maximum number of alerts (default 50 alerts), the interval over which that count is tracked (default 60 seconds), and how long the rule is suspended (default 10 minutes).

TABLE 10.1 Controlling the Number of Tracked Alerts

Name	Registry Key	Type	Default
Maximum Alert Count	HKLM\Software\Mission Critical Software\OnePoint\Configurations\<*configuration_group*>\Operations\Agent\MaxAlertCount\	DWORD	50 (alert count)
Maximum Alert Count Interval	HKEY_LOCAL_MACHINE\Software\Mission Critical Software\OnePoint\Configurations\<*configuration_group*>\Operations\Agent\MaxAlertCountInterval\	DWORD	60000 (in microseconds)
Maximum Alert Suspended Interval	HKEY_LOCAL_MACHINE\Software\Mission Critical Software\OnePoint\Configurations\<*configuration_group*>\Operations\Agent\MaxAlertSuspendInterval\	DWORD	600000 (in microseconds)

The registry settings need to be made on the agents, rather than just the MOM management server. They can be made on an agent-by-agent basis and will only affect the local agent.

For the large client in the example, the Maximum Alert Count registry setting on all the domain controllers was changed to 500.

If MOM Reporting is installed, you can use the Operational Health Analysis report to check for event storms. For more information, see http://support.microsoft.com/kb/923103/.

Real World—Sizing the MOM Databases

A common question that comes up regarding sizing is "How do I build for performance if I have no idea how big the OnePoint database or the MOM reporting database (SystemCenterReporting) will be?" That is an excellent question.

Responses to this question typically vary from "dunno" to the more politically correct version of "dunno," which goes something like: "It depends on the number of agents that you will be using and the number of management packs that you will be deploying." Interesting, but not extremely helpful. At a high level this is what we have determined:

The OnePoint database can only scale from 300 megabytes (MB) to 30 gigabytes (GB). MOM requires that the database have a minimum of 40% free space, leaving you with a maximum of 18GB as usable space (30GB x .6), so it is not unusual to see 30GB databases. We have a client maintaining a 10GB database that monitors 250 servers, and another client with a database well in excess of 30GB. The size of the database is directly related to how much data is captured, how many systems are monitored, and how long the data is retained in the database.

The reporting database will be large compared to the OnePoint database—terabyte-sized reporting databases are not unheard of. We discussed information on sizing for the MOM operational database in Chapter 4.

Monitoring the OnePoint Database

As we discussed in Chapter 4, Microsoft provides the MOM 2005 Sizer as a planning tool for configuring your monitoring environment. The Sizer estimates the size of the MOM database and gives numbers for the database and the log file segments. Use the size specified by the MOM Sizer as a minimum size for the OnePoint database. Remember, the OnePoint database stores all event, alert, and performance counter information gathered by MOM.

Regularly monitor the size of the OnePoint database and its remaining free space. There are some key indicators to watch and tools available to assist in monitoring the OnePoint database usage. You can monitor the free space of the MOM database within the SQL Enterprise Manager by checking the properties of the OnePoint database. You can also use SQL Query Analyzer to run the sp_onepointfreespace stored procedure, which reports the OnePoint free data space percentage. (If running SQL Server 2005, use SQL Server Management Studio to check database properties and run the stored procedure.)

The MOM 2005 management pack includes rules that monitor the available space in the OnePoint database and alert you when the remaining free space reaches specific thresholds. These rules are found in the MOM Administrator console under Management Packs \ Rule Groups \ Microsoft Operations Manager \ Operations Manager 2005 \ Server, and generate a warning alert if free space is less than 40% and an error alert when free space is under 20%.

Additionally the MOM database should not be set to automatically grow in size (autogrow). If the database is configured to autogrow, MOM generates an alert using the Management Packs \ Rule Groups \ Microsoft Operations Manager \ Microsoft Operations Manager 2005 \ Database \ Event Rules \ MOM Database State Monitoring rule.

OnePoint and Autogrow

We often are asked why the MOM 2005 database should not be set to autogrow. There are three primary reasons for this:

- A lock is placed on the database during the autogrow process. MOM 2005 is constantly reading and writing information to the OnePoint database. If the database is locked these reads and writes will fail and cause issues within MOM.
- If autogrow is set the OnePoint database could grow to exceed 30GB, which puts it beyond the supported boundaries of the database.
- Microsoft does not support autogrow for the MOM database.

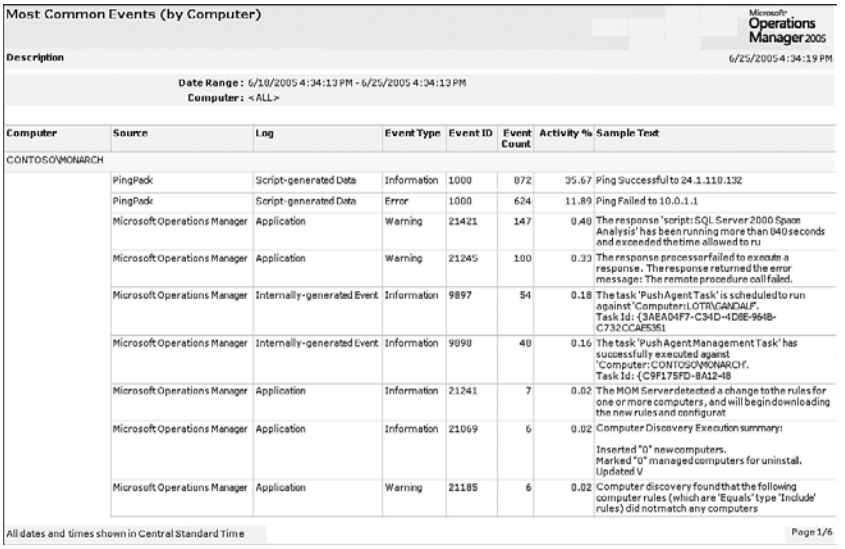
Monitor the Events Being Generated Generated events are often overlooked and can fill up the MOM database quickly if it is not being monitored. For example, MOM can collect all security events from the Security event log. If you add a domain controller as a managed agent and success auditing is enabled on that domain controller, there could literally be thousands of events inserted into the OnePoint database in a short amount of time. A large number of events will also generate additional network traffic; when a management server and database server are on different WAN segments this may represent a significant volume of network traffic.

If a management server and database server are at the same physical location they are most likely running on a LAN and are linked with a 100-megabyte or 1-gigabyte link. The bandwidth available on a WAN is generally much smaller with link speeds ranging from 64 kilobits per second (kbps) on a single-channel, integrated services digital network (ISDN) to 1.544 megabits per second (mbps) as the most common. The amount of time required to transfer the data will increase as the bandwidth of the network connection decreases. The latency (time required to travel from one system to another) on a LAN is minimal but increases significantly over various types of WAN links.

You can check the Events panel in the Operator console to identify whether specific events are generating a lot of information. MOM also has several reports indicating the number of events by computer or computer group, listing events by event ID as well as percentage of total for each event ID. The reports are found in the MOM Reporting console under Operational Health Analysis and are named the Most Common Events by Computer and Most Common Events by Computer Group. Figure 10.15 shows a sample Most Common Events by Computer report.

Both reports can be used to help determine which event or events are filling up your OnePoint database. You can use this information—specifically the event ID(s)—to research which rule or rules are generating these events.

Grooming Considerations Grooming refers to a scheduled process that deletes data from the database and automatically resolves alerts. If data is not being groomed, the OnePoint database eventually runs out of space. As discussed in Chapter 8, "Post-Installation Tasks," by default the grooming occurs daily at 12:00 a.m. by the *MOMx Partitioning and Grooming* SQL job.



Most Common Events (by Computer)

Microsoft Operations Manager 2005

Description 6/25/2005 4:34:19 PM

Date Range: 6/18/2005 4:34:13 PM - 6/25/2005 4:34:13 PM
Computer: <ALL>

Computer	Source	Log	Event Type	Event ID	Event Count	Activity %	Sample Text
CONTOSO\MONARCH							
	PingPack	Script-generated Data	Information	1000	872	35.67	Ping Successful to 24.1.110.132
	PingPack	Script-generated Data	Error	1000	624	11.89	Ping Failed to 10.0.1.1
	Microsoft Operations Manager	Application	Warning	21421	147	0.48	The response 'script: SQL Server 2000 Space Analysis' has been running more than 840 seconds and exceeded the time allowed to ru
	Microsoft Operations Manager	Application	Warning	21245	100	0.33	The response processor failed to execute a response. The response returned the error message: The remote procedure call failed.
	Microsoft Operations Manager	Internally-generated Event	Information	9897	54	0.18	The task 'Push Agent Task' is scheduled to run against 'Computer:LOTR\GANDALF'. Task Id: {3AEA04F7-C34D-4D8E-9618-C732CCAF5351
	Microsoft Operations Manager	Internally-generated Event	Information	9099	48	0.16	The task 'Push Agent Management Task' has successfully executed against 'Computer:CONTOSO\MONARCH'. Task Id: {C9F175FD-8A12-48
	Microsoft Operations Manager	Application	Information	21241	7	0.02	The MOM Server detected a change to the rules for one or more computers, and will begin downloading the new rules and configurat
	Microsoft Operations Manager	Application	Information	21069	6	0.02	Computer Discovery Execution summary: Inserted "0" new computers. Marked "0" managed computers for uninstall. Updated V
	Microsoft Operations Manager	Application	Warning	21185	6	0.02	Computer discovery found that the following computer rules (which are 'Equals' type 'Include' rules) did not match any computers

All dates and times shown in Central Standard Time Page 1/6

FIGURE 10.15 The Most Common Events by Computer report.

Grooming Failure

If the grooming job fails, MOM notifies you using the Management Packs \ Rule Groups \ Microsoft Operations Manager \ Operations Manager 2005 \ Database \ Event Rules \ A MOM Grooming SQL Server Agent job failed rule, which creates a critical error alert. If you start receiving a critical error that the MOM Grooming SQL Server Agent job failed, the problem should be addressed quickly.

You will have a nonfunctional MOM environment if your database runs out of space.

In addition, the DTS job that transfers data to the MOM Reporting database must successfully complete before the grooming task deletes data; this safeguard prevents MOM from deleting information not already copied to the MOM Reporting database. The MOM 2005 management pack includes a rule to monitor the DTS job for errors, generating an error alert if the job fails. This rule is located under Management Packs \ Rule Groups \ Microsoft Operations Manager \ Operations Manager 2005 \ Server \ Event Rules \ MOM Reporting DTS Job failed to complete successfully.

If grooming is not working correctly, the OnePoint database continues to grow until there is not enough space available for indexing, which will slow performance of the MOM environment. As the database grows it requires more resources on the SQL Server to effectively access information within the SQL Server database. When it reaches the point where there is less than 40% of available free space the reindex job fails, which further degrades the performance of the server.

Increasing the Size of the OnePoint Database Because the MOM database should not be set to autogrow, you may need to manually increase the database size as you add more agents and management packs to your management group. Use the following steps to increase the size of the OnePoint database:

1. Stop the MOM service on each management server in your management group. This prevents MOM from trying to write data into the database while you are performing database maintenance.
2. Always verify that you have a good backup of the OnePoint database. (Remember Murphy's Law?—Whatever can go wrong will!)
3. Use the SQL Enterprise Manager (SQL Server 2000) or SQL Server Management Studio (SQL Server 2005) to modify the database properties. Navigate to the OnePoint database and then right-click and select Properties. Click on the Data Files tab (or the Files Page in Management Studio) to bring up a window similar to that displayed in Figure 10.16.

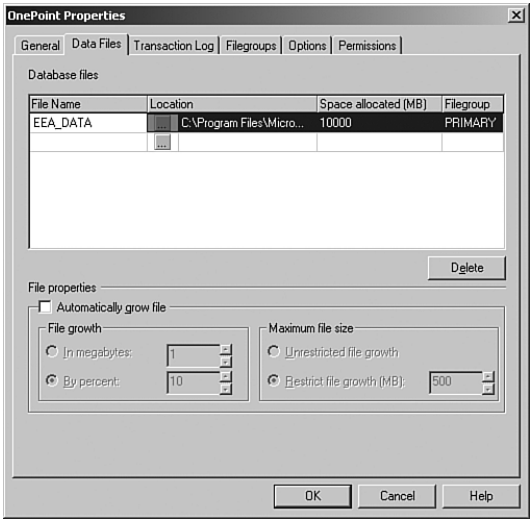


FIGURE 10.16 The data files properties for the OnePoint database.

4. To increase the space, type in the new value in the Space Allocated (MB) column. Remember that the total size specified cannot exceed 30GB. Click OK, and SQL Server will increase the size of the database to the new size you specified. (For Management Studio, the column is named Initial Size (MB). After you enter a new value, click on Add to increase the initial size.)

This process may take several minutes to complete depending on the size of your database. After SQL Server finishes expanding the database, restart the MOM service on your management servers.

Monitoring the Reporting Database

Size your reporting database to support how large it will likely be when it is fully populated. As discussed in Chapter 8, there is a direct relationship between the size of the OnePoint database and the MOM Reporting database. How big does the reporting database need to be? As a starting point, the Reporting database will be significantly larger than the MOM operational database because by default it stores data for 13 months. Details on sizing the MOM reporting database were discussed in Chapter 4.

Avoiding and Resolving Bottlenecks

The other major aspect for a high-performance MOM configuration is avoiding and resolving bottlenecks within your monitoring environment. You can use MOM itself to monitor and manage this! You should regularly review the state of each server providing components used by MOM.

Management Packs to Monitor MOM Components

To monitor your MOM environment for performance you will want to implement various management packs:

- The MOM 2005 management pack, which monitors the MOM server components, is loaded with the MOM installation—and you can't run MOM without it anyway!
- The Windows Base Operating System management pack checks for operating system–related performance bottlenecks (high CPU, insufficient memory, insufficient disk space, and so on). Additional concepts regarding the Base OS management pack are discussed in Chapter 15, "Managing the Operating System."
- The SQL Server 2005 management pack monitors the functionality of SQL database components and is discussed in Chapter 18, "Database Management."
- The Windows Server Clusters (MSCS) management pack monitors the functionality of your database clusters and increases uptime for the clusters, as discussed in Chapter 15.
- The Windows Network Load Balancing (NLB) management pack monitors the functionality of your reporting NLB cluster and is discussed in Chapter 15.
- The Web Sites and Web Services management pack monitors the performance of your reporting servers and is discussed in the following "Web Sites and Web Services Management Pack" section of this chapter.

Resolving bottlenecks is typically accomplished by either addressing the issue (adding CPU power, memory, or disk spindles; also known as *scaling-up the server*) or adding another server to your monitoring solution (*scaling-out*). For example, if your management server is experiencing high CPU utilization on a regular basis, you can either upgrade the server or add another management server and rebalance the load between those servers.

The management packs listed previously can assist you with monitoring the various components of your MOM solution and provide information to assist with avoiding and resolving bottlenecks in your environment. One management pack often overlooked when monitoring MOM is the Web Sites and Web Services management pack. This management pack monitors websites including those used by MOM.

Web Sites and Web Services Management Pack

The Web Sites and Web Services management pack assists in monitoring web server availability. Using Request Sequences, it can track website performance. MOM utilizes two websites: the Web Operator console and the Reporting console. Each Web console can be monitored by the Web Sites and Web Services management pack to assist in maintaining a high-performance web solution. Monitoring the MOM websites helps keep the consoles accessible.

Installing the Web Sites and Web Services Management Pack

The Web Sites and Web Services management pack requires more steps to install than other management packs:

- Download the management pack from the Web and run the .msi file to extract it; then import the management pack and/or reports as you would a standard management pack.
- Install the Background Intelligent Transfer Service (BITS) server extensions. If you are running Windows 2003, the BITS Server Extensions are available within Control Panel, Add/Remove Windows Components. If you are running Windows 2000, you can download BITS 1.5 from the Microsoft download center, http://www.microsoft.com/downloads.
- Run the Setup for the MOMWssMP.msi, which installs the Web Sites and Web Services Wizard. This wizard can also be installed on the administrator's desktop, which is preferred because then the "recording" of a request sequence takes place on a desktop rather than a production server.

Out-of-the-box, there is no monitoring built into the management pack to monitor either of these MOM consoles. However, by using the Web Sites and Services MP Configuration Wizard you can create a sequence of web requests (referred to as a Request Sequence), which can be used to monitor each of these sites. If these consoles are installed you will want to monitor both the Operator Web console and the Reporting console. We recommend monitoring each server that has a web-based console installed.

The Reporting console should also be monitored on each server where it is installed. In a highly redundant configuration this would be on an NLB cluster. For an NLB cluster configuration you would want to create Request Sequences for the NLB Cluster name itself, as well as for each node within the cluster (in our example this would be http://breckenridge/reports, http://breckenridge1/reports, and http://breckenridge2/reports).

Creating a Request Sequence The Web Sites and Services MP Configuration Wizard creates an entry on the Start menu within the Microsoft Operations Manager 2005 folder. To create a request sequence we run the wizard, shown in Figure 10.17.

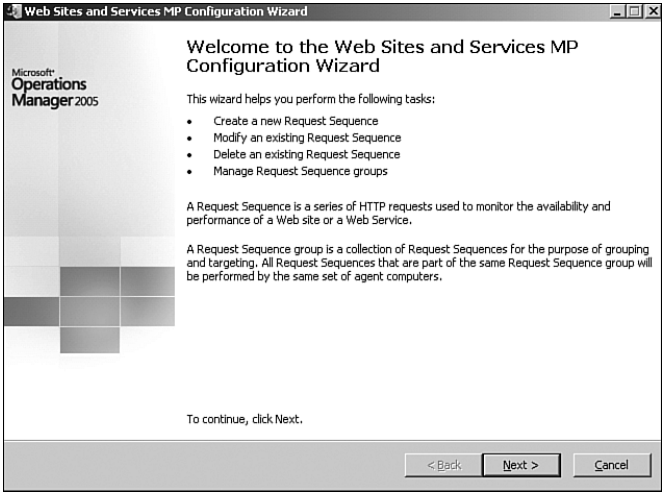


FIGURE 10.17 Starting the Web Sites and Services Wizard.

You will be prompted for the name of the management server (Monarch in our case), and after the wizard connects to the management server you can create, modify, or delete request sequences or manage request sequence groups. Because we are creating a new request sequence we will select the option to create a new request sequence.

Next, enter the name of the request sequence that you are creating. The wizard lists a set of options for how to create the request sequence. For simple request sequences, it is easiest to choose to Capture Web Site Navigation Using Internet Explorer as shown in Figure 10.18. This option opens up an Internet Explorer web browser and records the websites that are accessed until the capture is stopped.

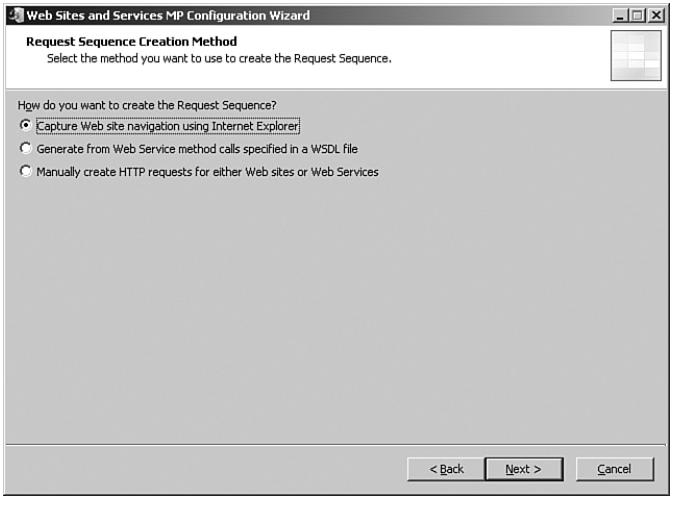


FIGURE 10.18 Capture Web Site Navigation Using Internet Explorer.

After the capture is complete you can add, edit, or delete the requests or reorder them within the list. Figure 10.19 shows an example of a simple request sequence to monitor the Operator Web consoles (Monarch, Keystone) and the Reporting consoles (Breckenridge, Breckenridge1, and Breckenridge2). After the list is finalized you can test the request sequence; if it is acceptable have the wizard save the changes to the management server. The management server will create a rule to run the request sequence.

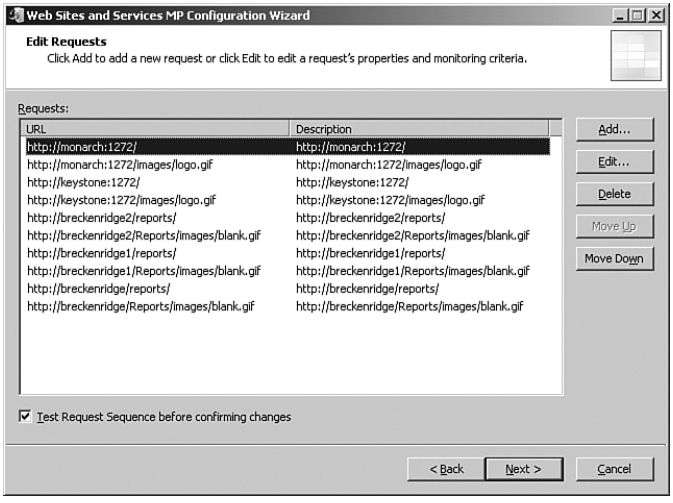


FIGURE 10.19 Creating a request sequence to monitor the Operator and Reporting consoles.

Reports The Web Sites and Web Services management pack also provides reports specifying the time required to access websites. The management pack assists you in identifying web server latency, which can help identify performance bottlenecks in the MOM web components. The management pack contains reports that assist in tracking performance of your Request Sequences. An example would be the Request Sequence Response Time report. This report graphs the response time in milliseconds for a specific request sequence. Figure 10.20 displays sample output, showing the response time of the MOM Reporting console request sequence.

Implementing a high-performance MOM configuration enables you to architect MOM to handle the load required of it. You can then utilize MOM's management packs to monitor all pieces of that architecture and address bottlenecks that occur.

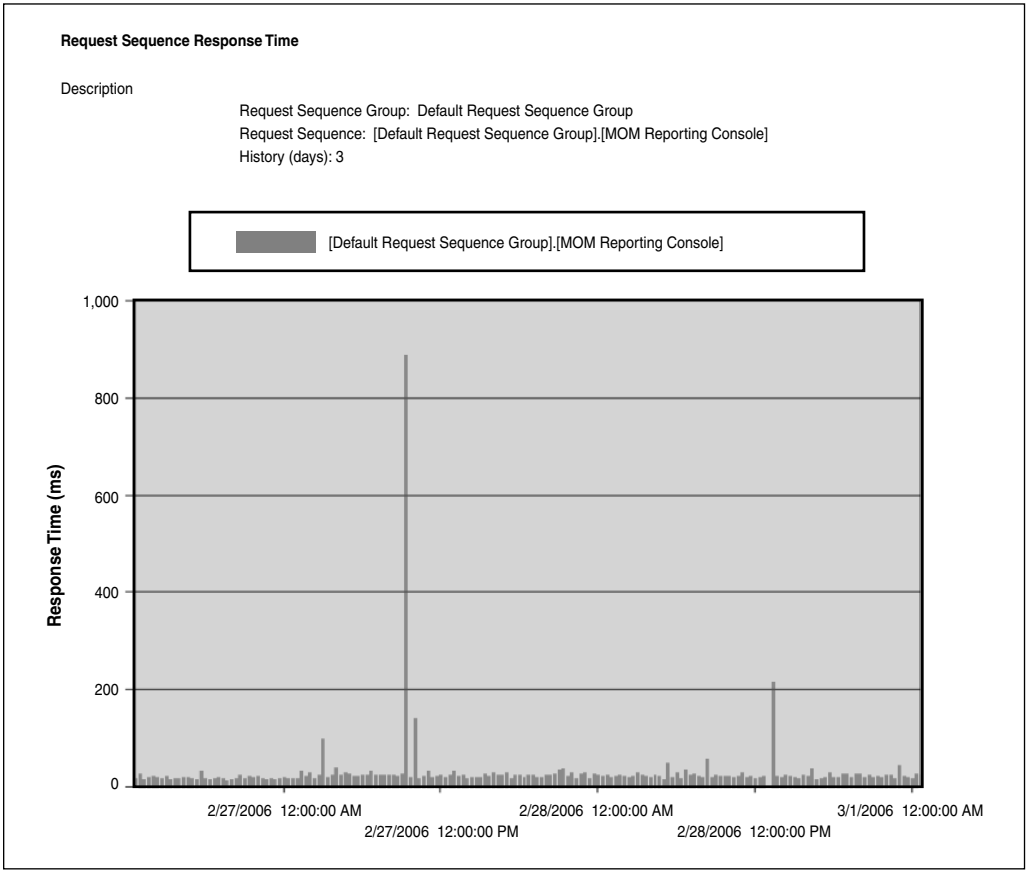


FIGURE 10.20 Web Sites and Services Request Sequence Response Time report.

Summary

This chapter focused on complex and high-performance configurations for MOM 2005. We reviewed considerations for achieving redundancy and providing a high-performance MOM configuration. We discussed various configurations that can be used for management servers, creating a fully redundant MOM 2005 configuration, and concepts for architecting MOM for performance. The next chapter discusses how security works in MOM 2005.

CHAPTER 11

Securing MOM

IN THIS CHAPTER

- MOM Security Groups
- MOM 2005 User Accounts
- Mutual Authentication
- Additional Security Considerations

This chapter examines different aspects of securing Microsoft Operations Manager (MOM). We discuss the security groups MOM uses, the accounts used by MOM 2005, and mutual authentication. We also consider how security for MOM works in multiple domains, how MOM monitors non-trusted domains, using MOM in an environment with firewalls, and securing communications.

MOM Security Groups

Microsoft uses group membership to control access to MOM 2005 resources. The management server installation creates the following security groups:

- MOM Administrators
- MOM Authors
- MOM Users
- MOM Service

These next two groups are also created as part of your MOM installation:

- SC DW DTS (Systems Center Data Warehouse Data Transformation Services)—This group is found on the server hosting the OnePoint database.
- SC DW Reader—This local group is created on the MOM reporting database server.

Group Type of the MOM Security Groups

The groups are local groups if the MOM components are installed on member servers and domain local groups when the components are installed on a domain controller.

MOM Administrators

The MOM Administrators group has full access to the MOM Administrator console and the MOM Operator console, giving members of this group the ability to perform any task in either console. MOM Administrators cannot perform reporting functions unless they are also members of the SC DW Reader group. Initially the MOM Administrators group has no members. Typically, members of your MOM Support team are added to this group.

Rights of Local Administrators

By default, members of the local administrators group on the management server have the same rights within MOM as members of the MOM Administrators group because the BUILTIN\Administrators group is added to the DAS Roles Security during installation. (The roles can be viewed under Component Services \ Computers \ My Computer \ COM+ Applications \ Microsoft Operations Manager Data Access Server \ Roles.) This access generally is not a security issue—because local administrators can always add themselves to the MOM Administrators group.

For organizations with high-security environments, the MOM 2005 Resource Kit includes a command prompt utility—UpdateDASRoles.exe—that removes local administrators from administrative access to MOM. The syntax for UpdateDASRoles is as follows:

```
UpdateDASRoles.exe /update
```

If necessary, you can later add the BUILTIN\Administrators back to the DAS COM+ application roles. Run the utility using the following syntax:

```
UpdateDASRoles.exe /undo
```

Run UpdateDASRoles on all MOM 2005 management servers and reboot for the changes to take effect. The utility's intent is to prevent local administrators from making inadvertent changes to MOM; it is not adequate as a security measure against a malicious local administrator.

MOM Authors

The MOM Authors group has full access to the MOM Operator console with access to the Operations and Management Packs nodes in the Administrator console. MOM Authors cannot change which computers are managed or how a computer is managed. By default, this group has no members upon initialization. The MOM Authors group typically contains individuals responsible for creating, customizing, importing, and exporting management packs.

Restricting Console Access

The security within the Management Packs node does not prevent individual management packs from being modified. A member of MOM Authors can modify rules in any rule group.

To prevent users from modifying specific rule groups, you can create separate management groups. Separate management groups are often implemented to control who can maintain security-related rules.

MOM Users

Members of the MOM Users group can view and modify alerts on the MOM Operator console, although they cannot perform runtime tasks. Use of the Administrator console is limited to opening the Operator console under the Operations node in the right-hand panel. The MOM Users group normally contains your Operations staff.

MOM Service

The MOM Service group is used for internal MOM services and processes. For example, the Data Access Service (DAS) account is added to this group when you install the MOM-to-MOM Product Connector. As an administrator, you would not modify this group unless changing the DAS account. The DAS account should be the only member of the MOM Service Security group.

SC DW DTS

The SC DW DTS group allows members to transfer data from the MOM (OnePoint) database into the MOM reporting database (SystemCenter Reporting). The group contains the Data Transformation Services (DTS) account you specified during the MOM Reporting setup process. As discussed in Chapter 6, "Installing MOM 2005," the DAS account is recommended as the DTS account. If you change the account used for DTS tasks, you must add that account to this group. This group is created on the system(s) containing the MOM OnePoint and SystemCenterReporting databases.

The SC DW DTS group is used exclusively by the DTS process that transfers data between the operations database and the reporting database. As such, it has read permissions on the operations database and read-write permissions on the reporting database. Do not use this for applications or users to access the reporting database or the operations database.

SC DW Reader

The SC DW Reader group is created when you install MOM Reporting. This group controls view access to the MOM reporting database, executes reporting functions, and performs the archiving (DTS) function. This group contains all accounts that can view the MOM reports.

This group has rights to read the SQL views in the reporting database and runs some of the stored procedures. Add the appropriate user accounts to the SC DW Reader group to grant them permission. You could also add a SQL Server user to the SC DW Reader role directly. The group is initially empty.

Adding Members to MOM Groups

There are two ways to add users to local groups:

- Using the Local Users and Groups system tool within the Computer Management console application.
- Using the command line, where the syntax would be:

```
Net localgroup "MOM Users" contoso\operator1 /add
```

  This command adds the operator1 account from the Contoso domain into the local MOM Users group. You can use this command to automate the maintenance process.

Monitoring Group Security

Review the MOM groups' memberships on a regular basis to ensure that those groups contain only the necessary user accounts.

There is a potential risk that the local groups on multiple management servers can get out of synchronization, with inconsistent rights across your MOM 2005 infrastructure. The next section discusses an alternative approach to adding users directly to each management server.

Using Active Directory Groups for Security Management

With local groups on the management server used to grant security access, potentially each management server in your management group could have a different view of the administrative model; that is, the user accounts membership in the local groups of each management server would differ. This decentralized administrative model could be considered a significant design weakness in MOM 2005.

To prevent unauthorized access to the MOM infrastructure, tightly manage and control your group membership. One approach is instead of assigning user accounts directly to the local groups on the management servers, add the user accounts to Active Directory groups and then add those groups to the appropriate local groups on all management servers. This strategy ensures a consistent administrative model across all management servers.

A sample naming convention could be

- Enterprise MOM Administrators
- Enterprise MOM Authors
- Enterprise MOM Users

You would create these groups in Active Directory and add them to the local MOM security groups on each management server. Next, add users to the appropriate Active

Directory groups, where they inherit appropriate rights to the management server. This technique uses the standard Windows security technique of adding users to global (or universal) groups. The global groups are placed in local groups that have access to the resources. This practice provides enterprise-level, role-based security management, and allows for straightforward auditing and administration of MOM 2005 security.

Using Security to Run MOM Tasks

MOM 2005 introduces runtime tasks and console tasks:

- *Console tasks* can only be run from the MOM Operator console. Common console tasks include Ping, Computer Management, and the Remote Desktop utility. Console tasks can be run by members of MOM Users, MOM Authors, and MOM Administrators, and use the credentials of the logged-on user. As discussed in Chapter 8, "Post-Installation Tasks," tasks are added to MOM by management packs or created using the Administrator console.
- *Runtime tasks* are tasks that run on a management server or agent-managed computers using the credentials of the appropriate Action account. MOM Authors and MOM Administrators can launch runtime tasks, but members of the MOM Users group cannot.

MOM 2005 User Accounts

MOM uses a number of service and "action" accounts. These accounts can be found on the management server and the managed computers. We will discuss the types of accounts, the rights and permissions they require, and how to change accounts used for particular functions.

Management Server Accounts

The following sections discuss the accounts associated with MOM 2005 management servers.

The Management Server Action Account

The Management Server Action account is used for a variety of functions including

- Installing and uninstalling agents (discussed in Chapter 9, "Installing and Configuring Agents").
- Running server-side responses on the management server.
- Running computer discovery.
- Gathering operational data from agentless computers.
- Running tasks issued from the MOM console. The account runs these tasks as one or more MOMHost.exe processes.

The Management Server Action account is specified during your MOM 2005 installation. Each management server has its own Action account; with multiple management servers you can specify the same Action account or use different accounts.

The Action Account and MOMHost.exe

The Host process (MOMHost.exe) runs under the Action account on the management server and the agents. This process and account is used by MOM 2005 to locally monitor, gather information about, and run responses on a computer. The management server also uses the Action account to deploy agents.

The account needs at least the following privileges on the management server:

- Member of the Users group
- Read access to the Windows event logs
- Member of the Performance Monitor Users group
- Granted the Manage Auditing and Security Log permission
- Granted the Allow Log on Locally permission

Although it can function with these minimum privileges, the Management Server Action account also deploys agents to remote managed computers, runs computer discovery, and updates agent settings. These actions all require administrative access to the managed computers, domain or forestwide.

Installing Agents The MOM 2005 Security Guide (available at http://go.microsoft.com/fwlink/?linkid=33035) suggests configuring the Management Server Action account as a local account with local administrative rights if the Action account will not automatically install agents.

The Install Agents Wizard allows you to use the Management Server Action account to install agents or to specify another account. If you specify the Management Server Action account, it must be a domain account with administrator rights on the target computers. Alternatively, you can configure the Management Server Action account as a low-privileged account and either specify credentials for installing agents when you use the Install/Uninstall Agent Wizard, or manually install agents.

Running Managed Code Responses You may specify an account other than the Management Server Action account for installing and uninstalling agents, but you cannot use a different account for performing any other of its functions. By default, custom response types (including managed code written using the .NET Framework) are excluded from executing because they can destabilize the management server. These actions are performed only by the Management Server Action account.

Executing Custom Responses

By default, MOM does not allow management servers to execute custom responses on behalf of the agent, although this setting can be changed using the MOM 2005 Administrator console, under Administration \ Global Settings \ Security.

Automating Computer Discovery MOM uses the Management Server Action account to perform Computer Discovery if discovery is configured to automatically install, uninstall, or upgrade agent-managed systems. Using computer discovery to automatically install agents also requires that the Action account be a Domain User with administrative rights on target agent computers. The account does not have to be a Domain Admin.

Configuring Agent Installation

MOM 2005 is initially configured to place discovered systems in a pending state and not automatically install, uninstall, or upgrade agent-managed computers. You can set MOM to automatically install, uninstall, or upgrade agent-managed systems in the MOM 2005 Administrator console, under Administration \ Global Settings \ Management Servers.

Having MOM automatically install, uninstall, or configure agents bypasses the approval process. This configuration should be carefully considered in regard to your change control process. Automatic agent installation could cause organizational issues if an agent is installed on a new server without going through Change Control and a manual approval process. If you start monitoring a system that is still being tested, your computer operators may get alerts for a server not yet ready for production monitoring.

Changing the Action Account/Password The SetActionAccount.exe utility allows you to determine the current Action account or change the account and/or password. SetActionAccount.exe is installed in the *%ProgramFiles%*\Microsoft Operations Manager 2005\ folder. The following parameters can be used with SetActionAccount.exe:

```
SetActionAccount.exe <management group name> <options>
Options:
-query
-set domain username [password]
```

Restart the MOM service after running SetActionAccount.exe for the changes to take effect.

Changes to SetActionAccount

The SetActionAccount.exe utility that shipped with MOM 2005 did not allow you to specify the Action account password with the `-set` parameter. The hotfix discussed in Microsoft knowledge base article 894464 (http://support.microsoft.com/kb/894464/) gives you the capability to specify the password using SetActionAccount and is incorporated in MOM 2005 Service Pack 1.

The corrected functionality enables you to script the execution of SetActionAccount and run it remotely. The original SetActionAccount utility prompted you to enter the password, so it had to be run locally when changing Action accounts or passwords.

The DAS Account

The DAS is a MOM 2005 Component Object Module Plus (COM+) application controlling access to the data in the OnePoint database. As shown in Figure 11.1, the DAS component acts as the interface to the database; all data inserted into the MOM database goes through the DAS. Data displayed in the MOM 2005 Administrator and Operator consoles also goes through the DAS application.

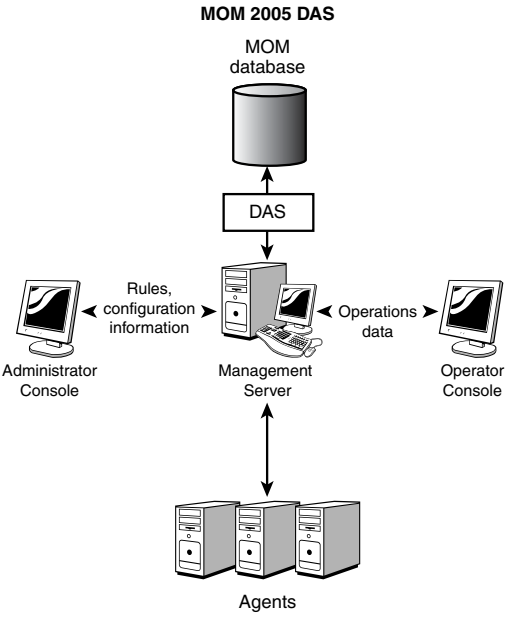


FIGURE 11.1 The MOM 2005 DAS.

The DAS account is specified during the management server installation, and the DAS COM+ application runs with the identity of the DAS account. The account must have the necessary permissions to the MOM database to read and write data. The installation program sets the necessary permissions and rights to the DAS account. The account does not require local administrator rights. The DAS account needs the following minimum rights, depending on the functions MOM is performing:

- Belong to the MOM Users security group—This is on each management server because the MOM Users group is a local security group.
- Have db_owner access to the OnePoint database—The DAS account needs full access to the operations database.

- Be a domain account or the Network Service account—Using the Network Service account is only possible on Windows Server 2003 systems.

  If the management server and OnePoint database are on the same system, you can also specify Local System (Windows 2000 and Windows 2003) or Local Service (Windows 2003 only).

- Have the Log on as a service right—This is only the case if the MCF is installed on that management server because the DAS account will need to run the MOM-to-MOM Connector service.
- Be a member of the SC DW DTS security group—This is only if the MCF is installed.
- Belong to the MOM Service security group—This is only if the MCF is installed.

The first three bullets are the base minimum requirements, and the latter three are required when the MCF is implemented. Using the Network Service account rather than a domain account requires some special configuration steps to grant the proper access.

Changes to the DAS Account in MOM 2005

For those of you who upgraded from MOM 2000 Service Pack 1 to MOM 2005, the original DAS account is retained as part of the upgrade, even though the DAS account in MOM 2005 requires fewer privileges than the DAS account does with MOM 2000.

The MOM 2005 DAS account no longer requires local administrator rights, the ability to log on as a batch job, create a token object, or act as part of the operating system. The MOM 2005 Security Guide discusses the changes to the DAS account.

Changing the DAS Account Changing the DAS account or the password it uses requires configuration changes to both SQL Server and the COM+ application. The following procedure changes the DAS to use the Local Service account, which is a lower privilege account available with Windows Server 2003. This example assumes that the management server and the OnePoint database are on the same server.

First grant the account the appropriate rights in SQL Server:

1. If you are using SQL Server 2000, open SQL Enterprise Manager and navigate to the Security folder for the appropriate SQL instance. Right-click the Logins folder, selecting New Login. On the General tab, type the name **NT Authority\Local Service**. Figure 11.2 displays the General tab of the SQL Server Login Properties box with the Local Service account.
2. Select the Database Access tab to grant the Local Service account the db_owner role for the OnePoint database. Figure 11.3 shows the roles specified for the database.
3. Click OK to add the new login to SQL Server.

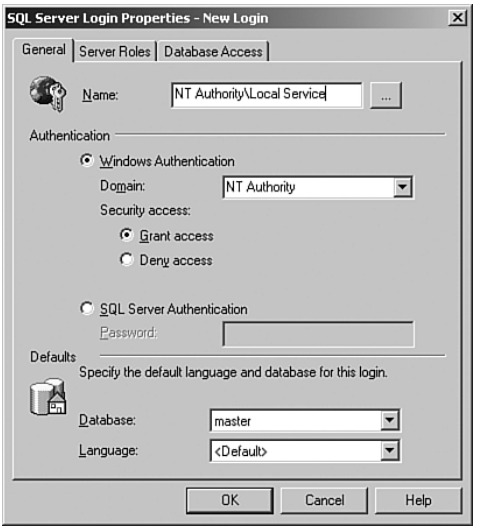


FIGURE 11.2 The General tab for new login in the SQL Server Enterprise Manager.

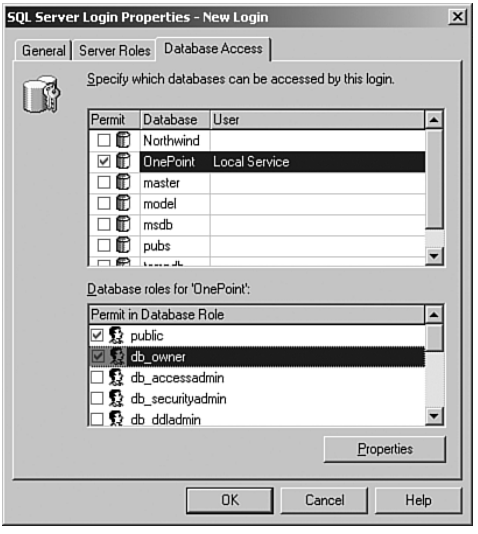


FIGURE 11.3 The Database Access tab for new login in SQL Server Enterprise Manager.

Adding the Local Service Account in SQL Server 2005

The process to add the Local Service account is slightly different for SQL Server 2005. Using SQL Server 2005 Management Studio, select Security in the Object Explorer; then right-click the Logins folder and select New Login to open the General page. Enter **NT Authority\Local Service** for the Login name. Select a default database of OnePoint, as shown in Figure 11.4.

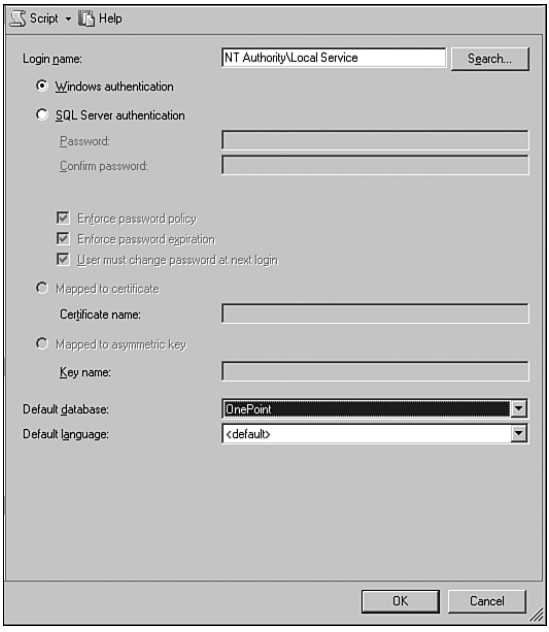


FIGURE 11.4 Adding a login in SQL Server Management Studio.

Now select the User Mapping page, displayed in Figure 11.5. Ensure that OnePoint with the NT AUTHORITY\Local Service is selected, and in the Database Role Membership for OnePoint section, check db_owner and public and click OK.

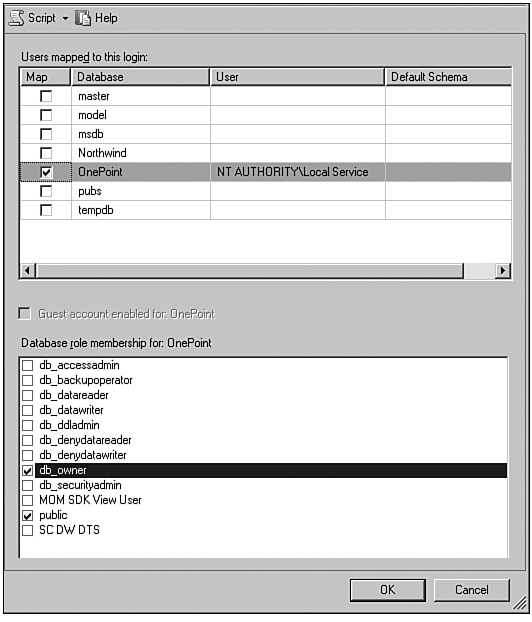


FIGURE 11.5 Granting db_owner access.

Now we will change the identity of the MOM 2005 COM+ application for DAS. Follow these steps:

1. Stop the MOM service on the management server. Although data is not written to the OnePoint database while the MOM service is stopped, the agents store the data in their local queue files until they resume communication with the MOM service on the management server. Using queue files minimizes data loss.
2. The DAS account is specified in Component Services under the Administrative Tools menu. Open the Administrative Tools icon from the Start menu and select Component Services. In the left pane, navigate to Component Services \ Computers \ My Computer \ COM+ Applications \ Microsoft Operations Manager Data Access Server, which is the DAS COM+ application.
3. Right-click on the application, choose Properties, and select the Identity tab. To change the account, select System Account and Local Service – Built-in Service Account. Figure 11.6 shows the configuration for using the Local Service account.

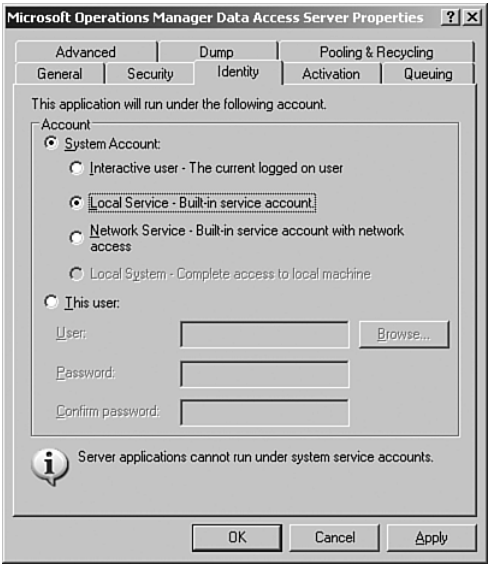


FIGURE 11.6 The MOM DAS COM+ Identity tab.

4. Click OK to confirm your changes.
5. Restart the MOM DAS COM+ application for the change to take effect. Right-click on the MOM DAS COM+ application and select Shut Down. Then right-click on the application again and select Start.
6. Now start the MOM service.

7. To verify that the DAS is operating properly, open the MOM Administrator console and confirm that there are no DAS errors. If there is data in the Administrator console, MOM is retrieving the data from the OnePoint database using the DAS COM+ application.

Incorrect DAS Configuration Log Errors

When the MOM DAS COM+ application is configured with an incorrect password, you may see a 1004 Distributed Component Object Model (DCOM) event in the System event log, or a 25613 MOM event in the Application event log. Verify that the correct account and password are specified for the DAS application.

Real World—Changing the DAS Account

If your goal is to use the lowest privilege account that gives you the most security, you can configure the DAS account to use a local user account, Local System, Local Service, or the Network Service account depending on your operating system and management server configuration:

- The DAS account can be a local account when the management server and OnePoint database are on the same server.
- The DAS account can also use the Local System account (Windows 2000/Windows Server 2003), or Local Service account (Windows Server 2003 only) if the management server and OnePoint database are on the same server.
- When the management server is on a separate server from the OnePoint database, the DAS account can be configured to use the Network Service account (Windows Server 2003 only) or Local System.

We recommend using the Network Service account as a best practice whenever possible because it offers minimal security exposure. The MOM 2005 Security Guide discusses the specific steps to change the DAS account to run under the Network Service context.

Password Update Utility You can also use a resource kit utility to change the DAS account. The MOM 2005 Resource Kit includes PasswordUpdater.exe, which changes a specified account or password on the following objects (provided that the password is already changed in Active Directory):

- Windows services
- COM+ applications
- Task Scheduler
- AT.exe
- Virtual directories in Internet Information Services (IIS) (Anonymous User and UNC User)

Use PasswordUpdater when changing the DAS account or its password. The utility includes a /t switch that tells you the changes it would make, allowing you to see what will actually change before making the change. The syntax for PasswordUpdater is as follows:

```
PasswordUpdater.exe <Options>
Options:
/s Server name
/f Server list file
/a Account name  (current DAS account)
/p password
/n New account name (for changing accounts option)
/x XML file path
/- Do not update these section names
/+ Update these section names
/t Tell me what would have changed
/I Inventory mode (attempts to find where passwords are stored)
/v Verbose mode
/r Restart services after update
```

If PasswordUpdater is run remotely from an administrative workstation targeting another server, a firewall cannot be in place between the workstation and target server.

Using the DAS Account and the MOM-to-MOM Product Connector

The MOM-to-MOM Product Connector (the MOMCONN service) uses the DAS account when communicating between management groups. If you change the DAS account, make sure that you do not impact the operation of the MOM-to-MOM Product Connector.

More on Connectors

The MOM-to-MOM Product Connector and the Microsoft Connector Framework are discussed in Chapter 19, "Interoperability."

The MOM Service Account

The MOM Service account communicates with the agents and runs the local agent on the management server. The account can use the credentials of either Local System (for Windows 2000 and Windows Server 2003 computers), or Network Service (with Windows Server 2003 systems).

The MOM Service process (MOMService.exe) runs under either the Local System account (.\LocalSystem) or the Network Service account (NT AUTHORITY\NetworkService), reducing the attack surface of the platform and easing the management burden. The process (and thus the account) is used to manage the MOM functions locally and to communicate with the management server.

The Local System account is available in Windows 2000, Windows XP, and Windows Server 2003, with high privilege levels on the local system. On a domain controller, the

Local System account privileges give it the equivalent to Domain Admin level privileges. The Network Service account is available only in Windows Server 2003. It has only the user-level access and presents the computer's credentials when authenticating.

Why Not the Local Service Account?

For those in the know, the account with lower privileges than the Local System account is the Local Service account. This has the same local privileges as the Network Service account and a smaller attack surface due to its inability to communicate outside the local computer. This seems a logical choice for the MOM Service account.

However, the requirement to communicate with the management server keeps the Local Service account from being be used because it has no rights to communicate outside the local computer. The Network Service account has that right.

Both accounts are preferable to using a domain-level account, which calls for significant rights on each computer and throughout the domain. A domain account would also require some level of maintenance because the password would need to be changed to keep it secure over time. The general recommendation for service account passwords is that they are changed at least once every three months.

Both the Local System and the Network Service accounts are self-managing, meaning that there is no password to set. This reduces the level of effort to maintain the services, which otherwise would require periodic configuration for password updates.

The Network Service account on Windows Server 2003 helps reduce the attack surface and security exposure of the MOM 2005 system by using a lower privilege account for its operations. By default, the installation deploys the MOM service to run under the Network Service account for the management server and the Local System account on managed computers. This is discussed in the "Agent Accounts" section later in this chapter.

You can find an additional discussion of built-in service logon accounts and their usage at http://go.microsoft.com/fwlink/?LinkId=50019.

Security Alert

The new service accounts available with Windows Server 2003 give you the capability of using a built-in account other than Local System. The Local System account on a domain controller has access to the Directory Service; if the account is compromised, access may be opened to the entire domain. Using the Network Service account, which has reduced privileges more like a user account, can help safeguard against attacks.

When the Action account uses the security credentials of a domain account, the MOM Service process (MOMService.exe) is installed using Network Service on member servers on Windows Server 2003 systems and Local System on domain controllers. For security reasons, you may want to reconfigure the MOM service on your domain controllers to use the Network Service account.

Watch the Account Used for the MOM Service!

The MOM service will not start unless it is running as either Local System or Network Service. Microsoft does not support changing the credentials to any other account.

Advantages of Using Built-In Accounts

Built-in accounts are maintained by the operating system and are not affected by password expiration policies. In addition, the passwords to these accounts are not exposed.

Real World—Running the MOM Service on Domain Controllers

The MOM service is installed using the Local System account on domain controllers. For security reasons, if you are using Windows Server 2003 we suggest you change the credentials used by this service from Local System to Network Service. Note that this can only be accomplished if the Agent Action account is not using the Local System account. If the Agent Action account is Local System, the MOM service must also run under the credentials of Local System.

Verify that the Network Service account has required NTFS permissions to the queue files under \Documents and Settings\All Users\Application Data\Microsoft\Microsoft Operations Manager 2005\<*management group name*>, and change the service definition used by the MOM service with the Services MMC (services.msc) application on the management server. Figure 11.7 shows a sample listing of the queue files and NTFS permissions for the Network Service account.

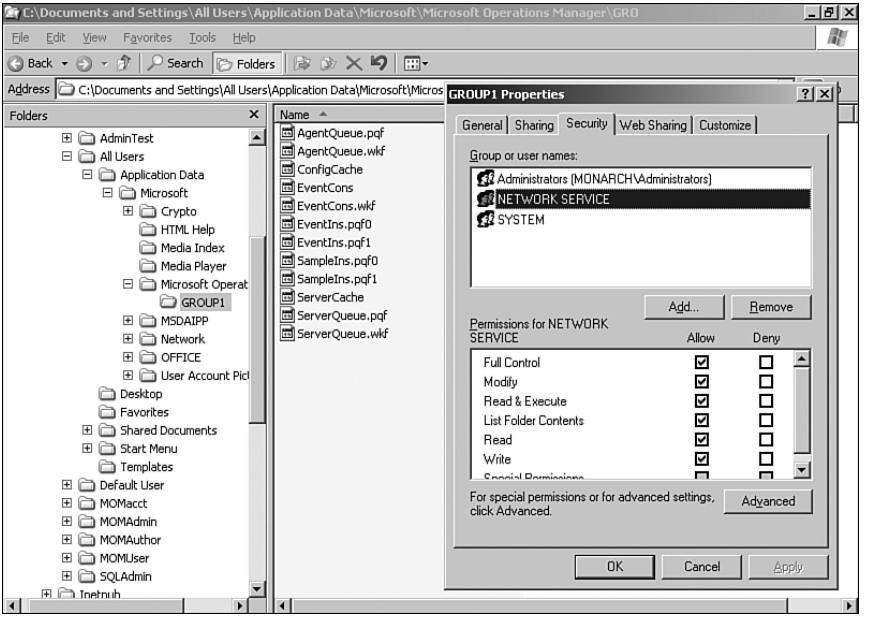


FIGURE 11.7 Queue file permissions for the Network Service account.

We suggest checking the MOM 2005 Release Notes for other potential changes to security settings when modifying services to use the Network Service account.

Agent Accounts

The next sections discuss the accounts used with MOM agents. MOM agents use an Agent Action account and a service account.

The MOM Agent Action Account

The MOM Agent Action account runs responses such as scripts or managed code responses on the managed computer. It is also used to gather performance data and events information from the managed computer. The MOM Agent Action account uses Local System by default, although you can use a lower privilege account for the Agent Action account. On Windows 2000 agents, the account must be a member of the local Administrators group. On Windows Server 2003 agents, the account must have at least the following privileges:

- Member of the local Users group
- Member of the Performance Monitor Users group
- Manage auditing and security log user right (SeSecurityPrivilege)
- Allow log on locally user right (SeInteractiveLogonRight)

Given the rights most likely needed for the managed computer's Action account, it makes sense to use the credentials of Local System. This account is the default option when installing the agent, although you can specify another account if you want. The MOM service uses the credentials chosen for the Action account.

Securing the Agent Action Account

You can use a local account for the Agent Action account. We recommend configuring a local account to help minimize the threat of an attack if the password is discovered.

Customizing the Agent Action Account for Specific Management Packs

Each management pack has different requirements for minimum privileges for the Agent Action account. Read the related management pack guide to determine the necessary privileges on the managed agent.

For example, if the agent for which you are configuring the Agent Action account is an Exchange server and a domain controller, you will need to combine the privileges necessary for each management pack to make sure that the Agent Action account has the appropriate rights to support all of the management packs that apply to it.

When you install the agent on a managed computer, you must specify the security credentials to use for the Action account on that computer:

- If you choose the default (Local System), the installation configures both the MOM Service and MOM Host processes to run under the Local System account.
- If you choose a domain account, the installation configures the MOM Service process to use the Network Service account and the MOM Host to use the specified domain account.

This is a bit quirky because the MOM Service process should always use the Network Service account.

Table 11.1 summarizes the results of the Action account choice on the agent.

TABLE 11.1 Resulting Process Accounts Based on Action Account Choice

Action Account Chosen During Install	MOM Service Process	MOM Host Process(es)
Local System account	Local System assigned	Local System assigned
Domain account	Network Service assigned	Domain account assigned

Within the registry of the managed computer, each management group has a separate set of keys and separate set of values for the Action account credentials. The management group key on the managed computer is HKEY_LOCAL_MACHINE (HKLM)\SOFTWARE\Mission Critical Software\OnePoint\Configurations\<*management group*>, and the two keys are ActionIdentityMode and Cache. There is also a separate <*management group*> entry for each management group the computer reports to. The value of ActionIdentityMode indicates the credentials used:

- If the ActionIdentityMode is set to 0, the MOM Host process uses the same account as the MOM Service process. The installation program sets the account to Local System (because Network Service does not have enough access rights).
- If the ActionIdentityMode is set to 1, the MOM Host process gets its credentials from the Cache registry value, and the MOM Service process uses the Network Service account.

The architecture allows each MOM Host process to set the appropriate Action Account credentials for the management group in the registry. This allows a common MOM Service process with a multitude of MOM Host processes to have different security credentials for each management group the managed computer reports to.

For example, say that there are two management groups in an organization, one for the group in Information Technology (IT) responsible for the Windows operating system and one for the group in IT responsible for the Exchange system. Although the Windows operating system management group could easily use Local System for its Action account,

the Exchange management group will need more access rights to gather Exchange-specific information and generate synthetic transactions.

Using the ConfigActionAccount Utility The MOM 2005 management pack is the only management pack automatically installed with Operations Manager. The MOM 2005 Resource Kit utility ConfigActionAccount.exe configures the Agent Action account with the minimum rights necessary for the MOM management pack.

ConfigActionAccount.exe is a standalone executable; it does not require the MOM Resource Kit to be installed on each managed computer. The syntax for ConfigActionAccount is as follows:

```
ConfigActionAccount.exe <user> <options> /user:domain\account
Options:
/mommp  - configure the minimum rights necessary for the MOM 2005 management pack.
/cleanup - removes the user from all rights granted by /nonmp
```

Using ConfigActionAccount

The `ConfigActionAccount` command works only with Windows Server 2003. You must be a local administrator on the managed computer to run this command.

Changing the Agent Action Account The SetActionAccount.exe utility used to change the Management Server Action account can also be used to view and change the Agent Action account. This utility is run on each agent. See the earlier section "Changing the Action Account/Password" for information on how to run the utility.

The SetActionAccount.exe utility cannot be used to change the Agent Action account to or from Local System. Reconfigure the agent to change the Agent Action account to Local System from a user account or vice versa (from Local System to a user account). For agent-managed agents, run Update Agents Settings from the MOM Administrator console and right-click on the agent-managed agent. For manually installed agents, modify the MOM 2005 Agent installation through Add/Remove programs in the Control Panel on each system.

The MOM Agent Service Account

Similar to the service account used with the management server, the agent service account is used when communicating with the management server and running the agent. The service account does not run responses such as scripts on the agent; the Agent Action account is responsible for that. The agent service account uses either the Local System account (for Windows 2000 or Windows Server 2003), or the Network Service account (Windows Server 2003 only). As with the management server service account, the agent service account will not start if it is not using the credentials of the Local System or Network Service account.

Default Configurations By default, agents installed by the management server run under the Local System account because the default Agent Action account also uses Local

System. As mentioned in "The MOM Service Account" section earlier in this chapter, access to the Local System account provides an attacker with greater ability to compromise your environment than the Network Service account, particularly on domain controllers, so you may want to change the credentials used by the Agent Action account.

MOM Agent Credentials If you specify a domain account or a local account other than Local System as the Agent Action account, MOM configures the agent service to run with the credentials of the Network Service account (assuming the monitored computer is running on a Windows Server 2003 system).

If the MOM Agent Action account is Local System and you change the MOM service to run under the Network Service account, the MOM agent will not function properly. The Action account will be unavailable and the agent will not be able to run responses. The Network Service account cannot load the Local System account as the Agent Action account when starting the MOM agent service. Change the Agent Action account to use the Network Service account in this case.

Further information on configuring agent security is available in the MOM 2005 Security Guide.

MOM Service Being Stopped

A common problem for some organizations is MOM agents stopped or disabled by unwitting or mischievous server administrators. MOM administrators then have to respond to missing heartbeat alerts and start up the MOM service using the update agent settings task, or worse, by logging in to the box and starting up the service manually. Even if the MOM administrator responds quickly, there can be gaps in data and potential outages.

The problem is that these server administrators are frequently local administrators for the managed computers, so they have rights to stop services by default and may need that right for other services in their day-to-day activities.

To help control this, you can create a simple Group Policy Object that locks down just the MOM service to a specific set of people that does not have to include local admins on that server.

You can create this Group Policy with the following steps:

1. Log in to a domain controller with an installed MOM agent. This allows you to see the MOM service as you are configuring the policy.
2. Type the command **mmc** at the Run prompt.
3. Open the Add/Remove Snap-in dialog (select File, Add/Remove Snap-in).
4. In the Add/Remove Snap-in dialog click Add, choose Group Policy Object Editor, and click Add.
5. In the Select Group Policy Object dialog, click Browse and select the OU, Site, or Domain that you want to target the policy at.

6. Either select an existing Group Policy Object that you want to modify or create a new one specifically for this by clicking on the New button.
7. Click OK. Click Finish. Click Close and then click OK.
8. Expand the tree as follows: Computer Configuration \ Windows Settings \ Security Settings \ System Services.
9. In the list of services in the Results pane, right-click on the MOM service and choose Properties.
10. In the properties dialog, check the Define This Policy Setting check box.
11. Select Automatic startup mode.
12. Click Edit Security.
13. In the Security for MOM Service dialog, lock down the access to the service however you want. You can even remove the local Administrators group. You can go so far as to not even allow them to see it! Make sure you set it up so that you still have access to see and manage the service in case you need to.
14. Click OK and then click OK again.
15. Wait for the next group policy update on the computers in the target scope that you created. If you want to force it immediately on a computer to test it out you can run **gpupdate /force** at a command prompt.
16. Repeat if necessary for other sites, domains, or OUs.

This process ensures that local administrators on the managed computers cannot stop the MOM service but can start and stop services as needed by their job requirements.

SQL Job Security

The database server uses a group of SQL Server Jobs to maintain the operations database. The owner of these jobs is automatically set to the user account that installed MOM 2005. These jobs require certain minimum permissions over the respective databases that the owner of the job must have to execute them properly (listed in Table 11.2).

TABLE 11.2 Permissions for Operations Database SQL Jobs

Job Name	Permissions
MOMX Partitioning And Grooming	db_datareader, db_datawriter, db_dlladmin, and execute for all stored procedures in the OnePoint database
OnePoint - Check Integrity	execute on xp_sqlmaint stored procedure in the master database
OnePoint - Computer Maintenance	db_datareader, db_datawriter, db_dlladmin, and execute for all stored procedures in the OnePoint database
OnePoint – Reindex	execute on master.xp_sqlmaint

TABLE 11.2 Continued

Job Name	Permissions
OnePoint - TodayStatisticsUpdateComputersAndAlerts	db_datareader, db_datawriter, db_dlladmin, and execute for all stored procedures in the OnePoint database
OnePoint - TodayStatisticsUpdateEvents	db_datareader, db_datawriter, db_dlladmin, and execute for all stored procedures in the OnePoint database
OnePoint - TodayStatisticsUpdatePerfmonRulesKB	db_datareader, db_datawriter, db_dlladmin, and execute for all stored procedures in the OnePoint database
OnePoint - Update Database	db_datareader, db_datawriter, db_dlladmin, and execute for all stored procedures in the OnePoint database
OnePoint - Update Statistics	dbo or sysadmin for the SQL Server
SCDWGroomJob	db_datareader, db_datawriter, db_dlladmin, execute for all stored procedures in the SystemCenterReporting database

You do not typically have to change the default owner unless database access is being restricted, in which case you can use Table 11.2 to guide you on what the minimum permissions should be.

Mutual Authentication

Mutual authentication is a new feature introduced with MOM 2005. All data sent between a management server and an agent is signed and encrypted by default. With mutual authentication enabled, the agent and the management server must authenticate each other before communications occur. Mutual authentication uses the Kerberos v5 authentication protocol.

Using Unencrypted Communications

Unencrypted communications (from MOM 2000) is not supported in MOM 2005.

Enabling mutual authentication helps mitigate a man-in-the-middle attack. A man-in-the-middle attack in these circumstances occurs when an attacker simulates a MOM agent or the management server, establishing communications with the management server or agent at the other end of the conversation, with the potential to perform a harmful action on the managed computer or management server.

The mutual authentication setting is configured as enabled or disabled in the MOM Administrator console, under Administration \ Global Settings \ Security. Mutual authentication is a management groupwide setting and cannot be set for only specific agents.

Mutual authentication is enabled during the MOM 2005 management server installation process when you answer Yes to the Active Directory configuration question. Figure 11.8 shows the Active Directory Configuration screen asking you whether your potential MOM agents are in Active Directory domains that trust each other.

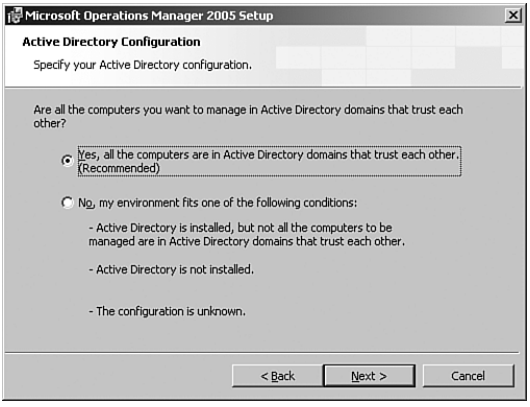


FIGURE 11.8 Specifying the Active Directory configuration.

When agents are installed by the management server (push installed), they inherit the current mutual authentication setting from the management group. When agents are manually installed, MOM prompts whether mutual authentication is enabled. Figure 11.9 shows the screen where you specify mutual authentication.

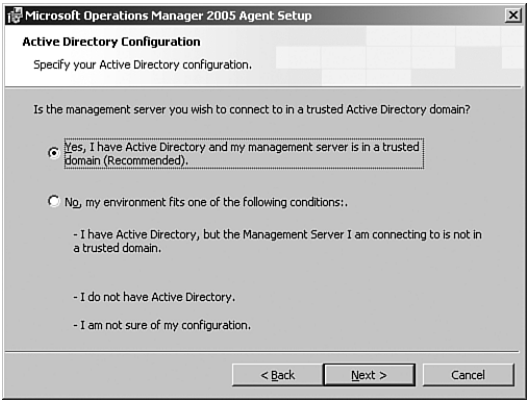


FIGURE 11.9 Connecting to a trusted domain.

Mutual authentication can be enabled or disabled using the MOM Administrator console. If the setting is changed, restart the MOM service on the management servers and agents for the change to take effect. You can also choose Update Agent Settings for the

agent-managed agents in the MOM Administrator console, under Administration \ Computers \ Agent-managed Computers. For manually installed agents that are not agent-managed, you would rerun the agent installation program and modify the current setup, using the Add/Remove Programs applet in the Control Panel on the managed server.

Avoid Errors When Resetting Mutual Authentication

If you change this setting, remember to recycle the MOM service on each agent to pick up the changes. If the MOM service is not recycled, error 26026 is generated indicating a mismatched configuration.

When Mutual Authentication Should Be Enabled

Mutual authentication is designed for a fully trusted Active Directory environment, including full two-way trusts between forests. Enable mutual authentication if there are two-way trusts across all domains between the agent's domain and the management server's domain, and none of the conditions exist that we describe in the following section.

When Mutual Authentication Should Not Be Enabled

Do not enable mutual authentication if any of the following conditions exist:

- MOM 2000 SP1 agents are reporting to the management group.
- Agents are installed on nontrusted clients, including workgroup clients.
- If you are supporting nontrusted domains and want to use mutual authentication, you can create separate management groups within the nontrusted domains and enable mutual authentication within each management group. The management groups can communicate with each other using the MOM-to-MOM Product Connector and the MOM Connector Framework. Security is provided via Secure Sockets Layer (SSL) encryption between the management groups. This process is discussed in Chapter 19.
- There are one-way trusts established across domains between the management server and the agents.
- One-way trusts exist across forests between the management server and the agents.

Using IP Security (IPSec)

If mutual authentication is not an option, you can use IPSec in lieu of mutual authentication.

- If there are NT 4.0 domains.
- If you are using the Released-to-Manufacturing (RTM) version of MOM 2005 and have a disjointed namespace. MOM 2005 SP1 supports disjointed namespaces and mutual authentication.

Tracking Communications Issues

If an agent cannot communicate with its management server because mutual authentication is preventing the communications, a 26023 event is written in the agent's Windows Application event log.

A good troubleshooting method when you have agent-to-management server communication issues is temporarily disabling mutual authentication to rule it out as the cause of the communication issue. Be sure to reenable mutual authentication when finished.

Additional Security Considerations

We will now discuss other security considerations with your MOM 2005 implementation. We will cover nontrusted domains, workgroups, agent proxying, and firewall and demilitarized zone (DMZ) configurations.

MOM and Nontrusted Domains

MOM 2005 will manage servers in untrusted domains. As mentioned earlier in the "Mutual Authentication" section of the chapter, mutual authentication cannot be enabled if agents in the management group reside in untrusted domains. However, you can push install agents from a management server to an untrusted computer. Let's look at the steps in this process:

1. Verify that the management server can resolve the Internet Protocol (IP) addresses of the computers in the untrusted domains. This may require adding name resolution using a host file or Domain Name System (DNS).

2. Create a discovery rule (or rules) for the computers in the untrusted domain. Figure 11.10 shows a computer discovery rule to discover all computers in the Coyote.com domain.

   Note the initial management mode is set to unmanaged, and the During Computer Discovery, Contact Each Computer to Verify It Exists option is not checked. This prevents MOM from trying to contact the computer in the untrusted domain.

3. After creating discovery rules created for the untrusted domain, you are ready to run computer discovery. Right-click on the Management Servers node under Administration \ Computers in the Administrator console and select Run Computer Discovery Now.

   Running discovery places the computers from the untrusted domains into the Unmanaged Computers node in the Administrator console.

4. In the Unmanaged Computers node, select the computer on which you want to install the MOM agent, right-click, and select Install Agent to launch the Install Agent Wizard.

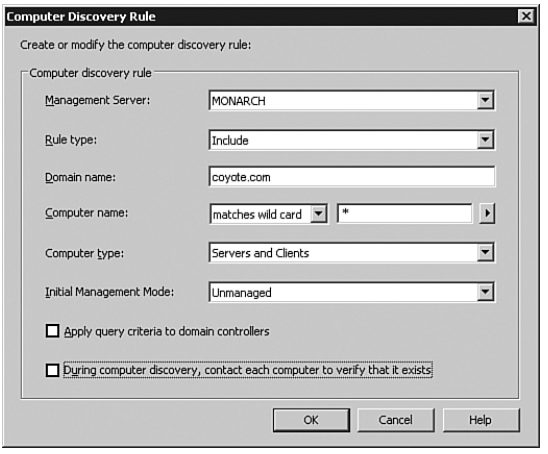


FIGURE 11.10 A discovery rule for nontrusted domain agents.

5. The second screen in the Install Agent Wizard dialog prompts you for an account that will allow you to install the agent. Enter an account from the untrusted domain with local administrator rights to the computer on which you are installing the agent by selecting Other, and enter the account that will install the agent. Figure 11.11 shows the Agent Installation Permissions screen where the account is specified.

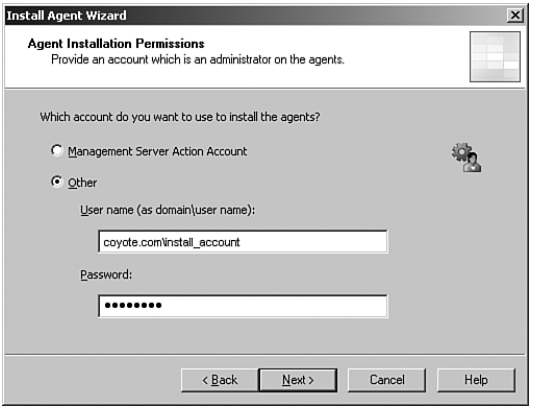


FIGURE 11.11 The Agent Installation Permissions screen within the Install Agent Wizard.

In this example, we use the Coyote.com\install_account for installing the MOM agent.

Manually Installing Agents

You can also manually install agents from untrusted domains.

Real World—Additional Capabilities in Nontrusted Domains

The MOM Administrator and Operator consoles can be launched from computers in nontrusted domains via proxy accounts (Windows 2003 computers) using the Stored User Names and Passwords feature or using the User Accounts capability (Windows XP computers). You must add the appropriate credentials for the domain with the MOM management server and database.

As discussed in the "Management Group Across a Firewall" section later in this chapter, you can install a separate management group in the untrusted domain and use the MOM-to-MOM Product Connector (MMPC) to communicate with other management groups. The MMPC is discussed in Chapter 19. Installing a management group in the untrusted domain also gives you the ability to enable mutual authentication.

MOM and Workgroup Support

Supporting agents on workgroup computers is similar to that of agents in untrusted domains. Agents can be manually (push) installed to workgroup computers; the only noticeable difference is that the workgroup name is substituted for the domain name in the discovery rules for the workgroup computers. The NetBIOS protocol must be enabled on the management server to allow for successful name resolution of the workgroup computers.

You cannot install a MOM management server or MOM database server on a computer that belongs to a workgroup; these roles must be installed on a member server or domain controller. In addition, mutual authentication cannot be enabled when managing agents in workgroups.

Agent Proxying

MOM 2005 supports agent proxying. Proxying is the capability for an agent to relay or forward information from other computers or network devices to the management server. Disabling agent proxying prevents spoofing by an attacker pretending to an agent because the management server matches information sent from the agent to a known agent name before accepting the data. Agent proxying is disabled by default.

Agent proxying is configured in the MOM Administrator console under Administration \ Global Settings \ Agents \ Security. Although this is a global setting, you can set agent proxying on an individual agent basis with an agent override.

To override the global setting and enable agent proxying for specific agents, perform the following procedure:

1. Navigate to Agent-managed computers in the MOM 2005 Administrator console, under Administration \ Computers \ Agent-managed Computers.
2. Right-click on the agent and select Properties.
3. Select the Security tab and uncheck Use Global Settings.
4. Uncheck the box that prevents the agent from using agent proxying.

You will need to perform this procedure for each agent for which you want to allow agent proxying.

Agent Proxying and Mutual Authentication

Agent proxying is only disabled if mutual authentication is enabled. Although you can disable agent proxying by checking the box in the Security tab, if mutual authentication is disabled, agent proxying is enabled.

A number of management packs use agent proxying. For example, the Active Directory Management Pack requires agent proxying for the client-side monitoring feature. The File Replication Service (FRS) management pack also requires agent proxying for monitoring replica members.

Suggested Setup for Agent Proxying

We suggest that you globally disable agent proxying and enable it as needed for individual agents.

Firewall Considerations

MOM 2005 supports both agents and management groups across a firewall. Mutual authentication is supported across a firewall when there are two-way trusts across all domains or forests between the management server and its agents and the ports required for Kerberos authentication are open.

Agents Across a Firewall

The MOM agent communicates with its management server over Transmission Control Protocol (TCP) port 1270 and User Diagram Protocol (UDP) port 1270. TCP port 1270 is used for all communication other than heartbeats, which are transmitted from the agent to the management server using UDP port 1270.

Using Port 1270

Port 1270 is the default management server-to-agent communication port. The port is configurable in the MOM Administrator console, under Administration \ Global Settings \ Communications. You cannot specify different port numbers between the TCP and UDP ports for client communications.

Because MOM's client push installation uses Remote Procedure Calls (RPC), agents must be manually installed and upgraded across a firewall or on a firewall server. When you manually install the MOM agent, make sure to select None for the agent control level. Figure 11.12 shows the Agent Configuration screen with None selected. An Agent Control Level of None tells MOM not to attempt to configure, install, or upgrade the agent. MOM

still performs discovery, placing the agent in the appropriate computer groups based on its computer attributes.

Restriction on Agentless Systems

Agentless systems are not supported on firewall systems including Microsoft ISA Server.

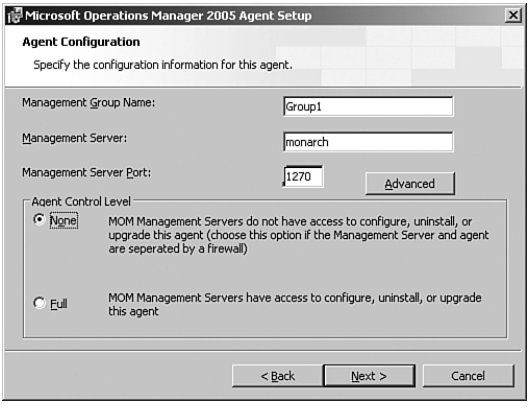


FIGURE 11.12 The Agent Configuration screen in the Manual Agent install.

The Reject New Agent Installations Setting

Uncheck the Reject New Manual Agent Installations option in the MOM Administrator console, under Administration \ Global Settings \ Management Servers \ Agent Install. This setting, enabled by default, does not allow newly installed manual agents to establish communications with the management server. Unchecking this option allows the agent to establish its initial communication with the management server. After all manually installed agents are deployed and communicating with their management server, recheck this box to prevent unauthorized manually installed agents from trying to communicate with the management server.

If the management server rejects a manually installed agent, a 26005 event is written to the Application event log for each agent, listing the IP address of the agent attempting communication with the management server.

Management Group Across a Firewall

You can install an entire management group on the other side of a firewall. You may decide to do this based on the number of agents across the firewall, DMZ configurations, geographic considerations, or trust considerations (situations where you want agents to communicate with mutual authentication enabled). Management groups across firewalls communicate via the MMPC, which uses TCP port 1271 by default. The MMPC is discussed in Chapter 19.

Restricted Use of Consoles with a Firewall

You cannot launch the MOM Administrator or Operator consoles across a firewall to communicate with a management group. Both consoles require RPC and DCOM ports to be enabled across the firewall. However, the MOM Web console will function in a firewalled environment. The MOM Web console listens on Hypertext Transfer Protocol (HTTP) port 1272 by default.

Management Server Across the Firewall from the Database Server

MOM 2005 supports installing a management server across a firewall from the MOM database server. The advantage to this configuration is it limits communications across the firewall to that between the management server and the database server, rather than the agents talking across the firewall to the management server. Additionally, agents can be automatically installed by the management server versus a manual installation when the management server is across the firewall from the target systems. This configuration requires opening firewall ports for Object Linking and Embedding for Databases (OLEDB) connections and DAS Authentication.

Configure the Firewall for OLEDB When the management server is across the firewall from the MOM database server, you need to open the OLEDB tunneling port, which is 1433 by default. The port number is configurable within SQL Server.

Configure the Firewall for DAS Authentication Separating the management server from the database server across a firewall requires configuration allowing the DAS account to be authenticated by the database server. Microsoft knowledge base article 832017 (http://support.microsoft.com/kb/832017/) discusses port requirements for Windows Server and Active Directory. The following ports are required for authentication:

- UDP port 53 to support DNS queries and dynamic registrations
- UDP port 88 to support Kerberos
- UDP port 123 to support Network Time Protocol (NTP)
- TCP port 135 to support RPC
- TCP port 445 to support Server Message Block (SMB)
- UDP/TCP port 389 to support LDAP

Port Requirements

Table 11.3 summarizes the port requirements when using a firewall between various MOM components. Remember that the Administrator and Operator consoles cannot be accessed through a firewall.

TABLE 11.3 MOM 2005 Firewall Capabilities

Component	Protocol and Port
Agent (agentless is not supported)	TCP/UDP Port 1270, discussed at http://support.microsoft.com/kb/904866/
MOM database to management server	TCP 1433 (Microsoft SQL Server connection)
Reporting database to MOM database	TCP 1433 (Microsoft SQL Server connection used for DTS)
MOM database to management server	OLEDB Tunneling Port 1433
Reporting database to MOM database	DTS Port TCP 1433
Reporting database to Reporting console	HTTP Port 80
Management server and Web console	TCP Port 1272
MMPC to MMPC	TCP Port 1271

Securing Your Environment

For a highly secure MOM environment, we suggest the following practices:

- Enable mutual authentication.
- Do not use a Domain Admin account as your Management Server Action account.
- Lock down the MOM groups (MOM Users, MOM Authors, and MOM Administrators).
- Disable agent proxying.
- Reject new manual agent installations.
- Use a low privilege Action account where possible. Each management pack has specific requirements for gathering data and executing responses. Remember that in a multihomed scenario each management group can select a different Action account.
- Make the Web console read-only. Edit the web.config file at %ProgramFiles%\Microsoft Operations Manager 2005\WebConsole\web.config and uncomment the `<add key="Readonly" value="true"/>` entry.

The recommended MOM configuration would also include:

- Do not automatically install or uninstall agents (automatic management).
- Use global settings as a default except where there is a specific need to override.

Communications Security

Microsoft designed MOM 2005 for secure communications, including protecting the integrity and the confidentiality of its communications:

- Protecting integrity ensures that the data transmitted is not tampered with or altered during transit.
- Protecting confidentiality guarantees that the data transmitted is not read in transit.

Both these aspects can be important if, for example, security data such as a user's login times or file access is sent from the managed computer to the management server and the operations database. You would not want the information either changed or viewed by just anyone on the network.

MOM 2005 not only leverages the security features of the Windows platform and applications, such as SQL and IIS, but also uses its own custom method. The security methods used by MOM 2005 include the following:

- Custom signing and encryption with mutual authentication—This MOM 2005–specific method encrypts and signs the traffic over a specific port for agent to management server communications. It also supports mutual authentication if the management server and agent are in the same Active Directory forest. This is configured in the MOM 2005 Administrator console.
- IPSec—Internet Protocol Security (IPSec) is a method of securing IP communications, supporting both confidentiality and integrity through encryption and signing of traffic. IPSec supports a wide array of cryptographic methods and algorithms. The Windows Server 2003 and Windows 2000 platforms include the IPSec protocol and support automatic deployment of IPSec. This is configured in the Windows operating system.
- SSL—Secure Socket Layer (SSL) Encryption uses certificates to secure traffic, typically browser-based traffic. SSL requires that certificates be installed on both sides of the communication channel and then uses asymmetric public key encryption to generate keys for high-performance symmetrical encryption. SSL is configured in the IIS Manager console.
- OLEDB Encryption—This is a security method built into the SQL server application. OLEDB Encryption uses SSL to secure the communication between SQL clients and the SQL server. OLEDB encryption is configured in SQL Enterprise Manager (SQL Server 2000) and SQL Server Management Studio (SQL Server 2005).
- SMB Packet Signing—SMB is the file transfer protocol used by Windows. SMB Packet Signing protects the integrity of the file transmission by digitally signing each SMB packet. This is configured in the Windows operating system.

Figure 11.13 shows the component communication diagram with the respective security methods. Note that all external communications can be secured through one method or another, ensuring that all MOM communications can be secure if needed.

Although these methods are all available, by default MOM 2005 only secures confidentiality and integrity of the communication from the agent to the management server using custom signing and encryption. The other methods require additional configuration. Table 11.4 summarizes the communications and their protection methods.

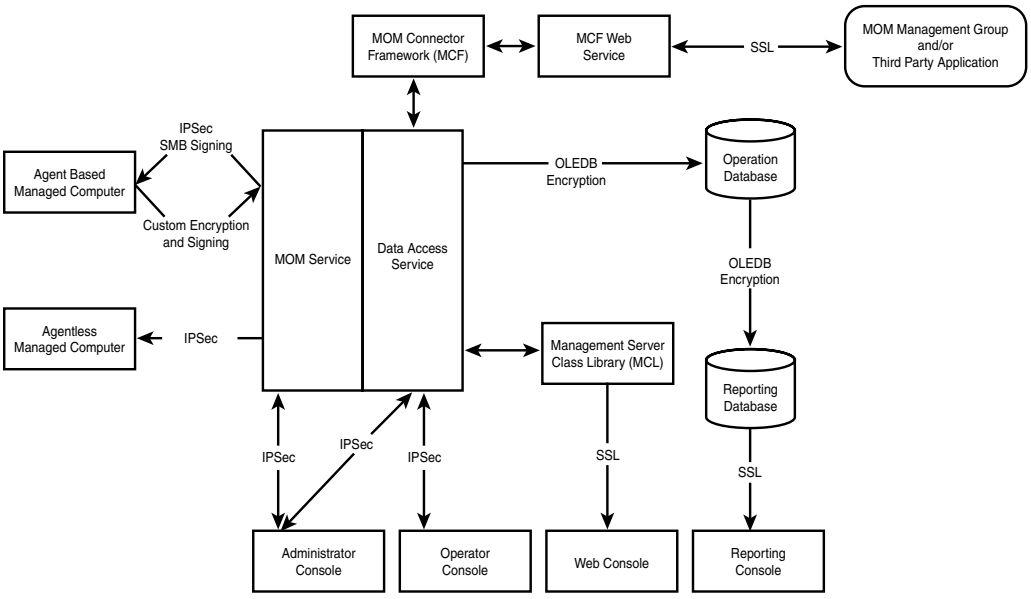


FIGURE 11.13 Component communications security methods.

TABLE 11.4 Communications Security

From	To	Protection Method	Default?
Agent	Management server	Signed and encrypted with mutual authentication	Yes
Management server	Agent	IPSec, SMB packet signing	No
Management server	Agentless	IPSec	No
Administrator console	Management server	IPSec	No
Operator console	Management server	IPSec	No
Reporting console	Reporting database	SSL	No
Web console	Management server	SSL	No
Management server	Operations database	OLE DB encryption	No
MOM-to-MOM connector	MOM-to-MOM connector	SSL	No
Connector	Third-party application	SSL	No
Operations database	Reporting database	OLE DB encryption	No

Each security feature is configured in its own respective area and is not mutually exclusive. For example, you might configure both IPSec at the operating system level and OLEDB encryption at the SQL Server level to secure the traffic between the management server and the database server. The downside is that each of these security methods has

some sort of performance penalty, and layering them adds to the overall penalty. It is important to not oversecure communications in such a way as to degrade the performance of your system. Security is always a balance between needs and costs, which can be expressed in a number of ways such as monetary cost, administrative complexity, maintenance, and/or performance costs.

Summary

This chapter looked at security groups installed by MOM and reviewed the service accounts that MOM uses, including reducing rights and changing the accounts and passwords. We also looked at mutual authentication and when it can and cannot be used. We concluded the chapter by looking at nontrusted domain considerations, workgroup support, agent proxying, DMZ implementations, firewall considerations, and communications security. Additional information on MOM security can be found in the MOM 2005 Security Guide, which can be accessed online at http://go.microsoft.com/fwlink/?linkid=33035 or downloaded from the Microsoft Download Center (http://microsoft.com/downloads) by searching for "MOM 2005 Security Guide."

The next chapter looks at backup and recovery techniques for MOM 2005 and also discusses disaster recovery planning.

PART IV

Administering MOM

IN THIS PART

This page intentionally left blank

CHAPTER 12

Backup and Recovery

IN THIS CHAPTER

All production systems should have backup and recovery procedures in place, and a Microsoft Operations Manager (MOM) infrastructure is no exception. Out-of-the-box, MOM 2005 does not include a backup process. If the OnePoint database becomes damaged through corruption or a hardware failure and you are without a database backup, you will have to reinstall the management group and re-create the database. This creates all kinds of headaches.

Re-creating the database without the ability to restore what was previously there means that you lose all customization and operational data collected in the database. If MOM Reporting is installed and you lose the ReportServer and SystemsCenterReporting databases, you lose the reporting data you have accumulated in SystemCenterReporting, plus MOM report definitions and report customizations, which are stored in the ReportServer database. This potential data loss makes it critical to create a backup and recovery plan for your MOM 2005 implementation.

This chapter discusses backup and recovery strategies for MOM. We also look at a methodology for handling large report databases and requirements for disaster recovery planning.

Roles of Key MOM Files and Databases

Backing up appropriate files and databases in a timely manner facilitates minimal data loss if there is a catastrophic failure in your MOM infrastructure. You should include the following files and databases in your backup strategy:

- The OnePoint database—This is MOM's operational database and is the most important item to back up. If you lose this database due to a hardware failure or corruption and do not have a database backup, you will have to reinstall the management server and re-create the database, losing all rule customizations, discovery rules, and operational data collected. This database is shared among management servers within a management group, and must be backed up for every MOM management group.
- The SystemCenterReporting database—This database stores archived operational data, which is used by SQL Server Reporting Services for trend analysis and performance tracking. Based on the amount of data you are collecting, this database may be large. If you have not installed MOM Reporting, your management group does not include the SystemCenterReporting, ReportServer, or ReportServerTempDB databases. The SystemCenterReporting database can grow to a relatively large size and thus require special handling.
- The ReportServer database—This database stores the report definitions used for MOM Reporting and is updated when new reports are defined or definitions of existing reports are changed.
- The ReportServerTempDB database—The only reason to back up ReportServerTempDB is to avoid having to re-create it if there is a hardware failure. If there is a hardware failure, you do not need to recover the data in the database, but you will need the table structure. If you lose ReportServerTempDB, the only way to get it back is by re-creating the ReportServer database.

Backups for MOM 2005 Workgroup Edition

MOM 2005 Workgroup Edition does not include reporting functionality, so you would not need to back up the SystemCenterReporting, ReportServer, or ReportServerTempDB databases.

- The master database—This is a system database, recording all information used by a SQL Server instance—including database file locations, configuration settings, and login account information. This database should be backed up whenever there is a change to your SQL Server configuration.
- The msdb database—The msdb is also a SQL Server system database, containing scheduled tasks information for jobs, including regularly scheduled database backups and the SQL MOMx grooming job.
- Management packs and reports—Management packs contain rules and information pertaining to how MOM monitors applications, services, and devices. The management packs are stored in the OnePoint database, which you should back up as part of your standard procedure. We recommend separate backups of management packs for the granularity to import them directly into MOM when necessary and to save a self-contained copy of your rule customizations. Instances of importing management packs could include rolling back changes to a management pack or moving a management pack from a development to production environment.

Report templates are stored in the ReportServer database. As with management packs, we recommend separate backups of any reports you have created or customized.

- File transfer server files—Although not technically part of your MOM environment, the files used for file transfer server responses should be backed up. File transfer server files include log files transferred from an agent and software updates transferred to an agent for installation, such as the MsSecure.cab used by the Microsoft Baseline Security Analyzer (MBSA) management pack.
- Custom files—These include the ManualMC.txt file, which is typically found on each management server and contains a list of manually installed agents. Other custom files are .msc files created for custom MOM Administrator consoles, .omc files for custom MOM Operator consoles, and the encryption keys for SQL Server Reporting Services.

In addition to identifying required files for backup, you should also establish a regular backup schedule. Tables 12.1 and 12.2 give suggested time frames for backing up significant databases and files used by MOM 2005.

TABLE 12.1 MOM Databases with Recommended Backup Schedule

Database	Name	Type of Data	Recommended Backup Schedule
Operations database	OnePoint	This database contains the majority of the MOM configurations, settings, and the current operations data. The loss of this database would mean having to completely reconfigure MOM and the loss of up to the previous 24 hours of operations data.	Daily
Reporting database	SystemCenterReporting	This database holds all the archived operations data and can be large. The loss of this database would mean the loss of all historical operations data.	Daily or Weekly
SQL Server Reporting Services database	ReportServer	This database holds all the report definitions, as well as cached report information and snapshots. The loss of this database would mean having to reimport reports and re-create subscriptions. Minimal impact.	Monthly
Master database	Master	This database is a SQL system database and records the system information for SQL.	Daily

TABLE 12.1 Continued

Database	Name	Type of Data	Recommended Backup Schedule
MSDB database	Msdb	This database is a SQL system database and holds all the scheduled jobs, some of which are critical for the proper functioning of MOM and the generation of MOM reports.	Daily

TABLE 12.2 Significant Files with Recommended Backup Schedule

File	Type of Data	Recommended Backup Schedule
Management packs and reports (.akm and .xml files)	Source files for management packs and reports. Enable more granular restoration than entire Operations database; also used for moving management packs and reports from one management group to another.	After changes to management packs or reports
File transfer files	Examples include MsSecure.cab used by the MBSA management pack.	As needed
Custom files	Customized console files, ManualMc.txt, and so on.	As needed

Reporting Database Backup Considerations

The sheer size of the reporting database presents potential backup issues. This database can potentially grow to a terabyte in size, which can take a long time to back up and restore. There may also be the need to maintain several of these large databases if you have many agents and choose to maintain archive databases for different months, quarters, or years, each with a size of 1 terabyte.

A sophisticated backup schedule that accommodates using archive databases would be to only back up the current reporting database (SystemCenterReporting) but retain online copies of archived versions. The archived databases were backed up when they were current, so all that is required is to maintain those tapes in long-term storage for as long as needed. This approach allows you to reduce the volume of data backed up on a daily or weekly basis, while still retaining long-term availability of the data via archive databases and long-term tape storage.

For example, we will consider a company monitoring 1,000 computers. It does not have third-party software with a SQL backup agent, so will use Microsoft SQL Server's backup capability. The company needs access to a year's worth of operations data, which results in a reporting database close to 2 terabytes (TB), which is outside supported limits and too large to easily back up directly to tape. In addition, a backup to a disk file requires equivalent storage on disk for the backup for a total of 4TB. This is too much storage as well.

However, operations data for a single quarter will be approximately 500 gigabytes (GB) or one-half terabyte. This amount is within the supported limits and within the capability of the tape backup system. The company decides to break up the reporting database into quarterly archives and accordingly set the reporting database grooming to groom data after a quarter. This configuration has been running for more than a year, so they have a steady state condition.

Figure 12.1 illustrates the steady state backup process. You can see that the current reporting database is available (SystemCenterReporting), as well as the four previous quarters of archived data (4Q2006, 3Q2006, 2Q2006, and 1Q2006).

- Step 1 backs up the reporting database to a disk file. This is an online backup, so there is no interruption in service.
- Step 2 backs up the backup file to tape. In the event of a disaster, the tape backup could be easily restored.

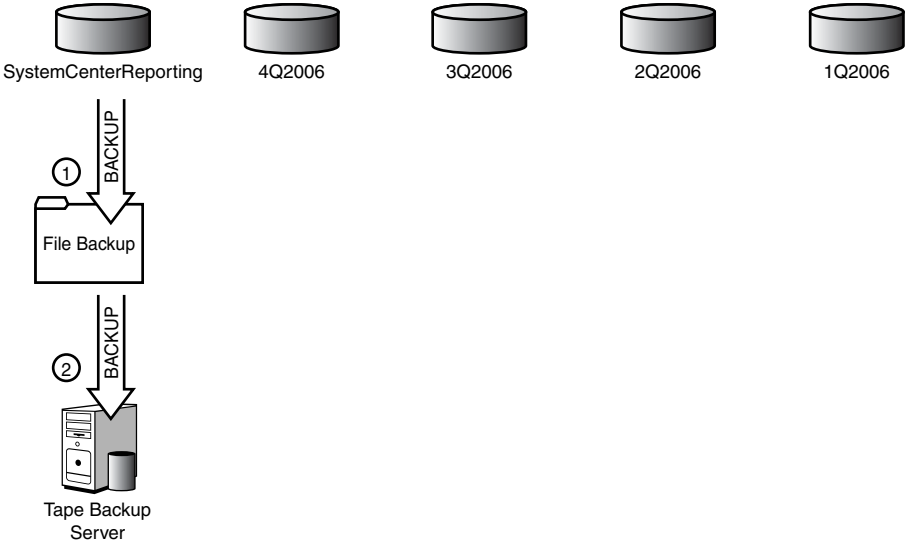


FIGURE 12.1 Steady state backup of reporting database with archives.

Note that that this process could take place weekly, daily, or even every 4 hours if necessary, with the process remaining the same. The amount of disk storage required is based on the size of the databases. Calculating size for a 500GB database with one quarter of data, the company will need disk storage to hold five databases (5 x 500GB) plus 500GB for the file backup. This is a total of 3,000GB or 3TB. Contrast this figure with the original 4TB storage requirement, and you can see we have conserved on disk storage as well. We also only need to back up 500GB at a time, rather than 2TB.

As usual, there is no free lunch. The catch is a certain amount of administrative overhead required to handle the backup process at the end of each quarter. This end-of-quarter backup process is a bit more complex and is shown in Figure 12.2. The following steps outline the process of transitioning backups at the end of 1Q2007:

1. First, the reporting database is backed up to a file. This is an online backup, so there is no interruption in service.
2. The backup file is then copied to tape. In the event of a disaster, the tape backup could be easily restored.
3. The backup file is restored to a new database storing data for that quarter (in this example, 1Q2007).
4. The database that is now outside the data retention requirement of one year (1Q2006) is deleted.
5. The tape backup of the reporting database—that is,—1Q2007, is replicated to long-term tape storage.

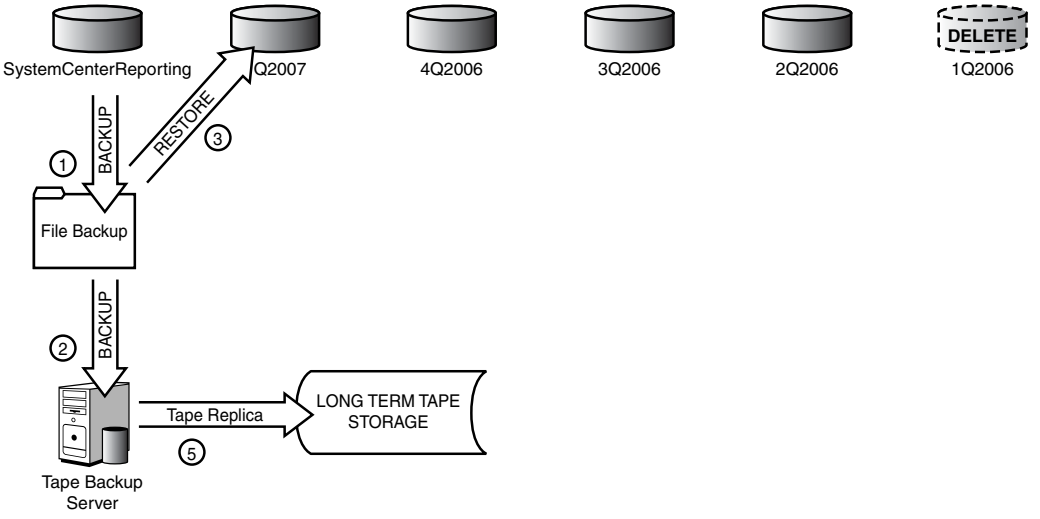


FIGURE 12.2 Quarterly backup of reporting database with archives.

These processes can be automated with scripts and jobs, or even run manually as end-of-quarter procedures. The overall process is flexible and can be adjusted to support monthly archives rather than quarterly. The advantage of monthly archives is that the backups are correspondingly shorter, but the report horizon will be shorter and only cover a single month.

Backing Up and Restoring the SQL Server Databases

Many Information Technology (IT) organizations have a database support group responsible for their Microsoft SQL database servers and in charge of backing up and restoring SQL Server databases. You should work with your database group to ensure that an appropriate backup and restore plan exists for your MOM databases. If you do not have a group

responsible for database backups, you will need to create your own backup and restore plan. This plan includes scheduling times for backups, identifying actual database files, and defining procedures for backing up and restoring those files.

Most enterprise backup implementations include a separate software module that can be installed to back up a SQL Server database while it is running. It is highly recommended that this type of backup agent be employed in your design to provide for online backups of the MOM databases.

An alternative solution is using SQL Server's backup feature to back up the databases to file and then back up the resulting files. This does not require a SQL backup agent and has the advantage of being very fast. The downside is that you need sufficient disk space to hold a backup the size of the entire database, which in the case of the reporting database can be large.

Database Backups

We will use SQL Server's backup component to back up the OnePoint database as an example of the process that you can use for the other databases used by MOM 2005. SQL backups are defined using SQL Server Enterprise Manager (SQL Server 2000) or SQL Server Management Studio (SQL Server 2005). For the OnePoint database, we should always perform a complete backup—not a differential backup—because MOM supports a simple recovery from a full backup only, not a forward recovery with the transaction log.

Types of Database Recoveries

Without getting too much into database technology, Microsoft SQL Server supports three types of recovery—full, bulk_logged, and simple. A *full* backup uses the database and transaction log backups for full recoverability. *Bulk_logged* uses minimal transaction logging for bulk load types of operations—if a recovery is necessary, those transactions must be reapplied. *Simple*, which is used by both the OnePoint and SystemCenterReporting databases, recovers the database without using the transaction logs as part of the process. The ReportServer database uses the Full recovery model.

The OnePoint database should be backed up daily. The following procedure defines a backup job for the SQL Server 2000 OnePoint database:

Backup and Restore Steps for SQL Server 2005

Microsoft added SQL Server 2005 support for the MOM 2005 operational and reporting databases in 2006. The SQL Server Management Studio screens are slightly different from those used in SQL Server Enterprise Manager for the backup and restore steps and will be shown separately.

1. In SQL Server Enterprise Manager, navigate to Microsoft SQL Servers \ SQL Server Group \ Local \ Databases \ OnePoint. Right-click on the OnePoint database, select

All Tasks, and then choose Backup Database, which brings up the main Backup screen shown in Figure 12.3.

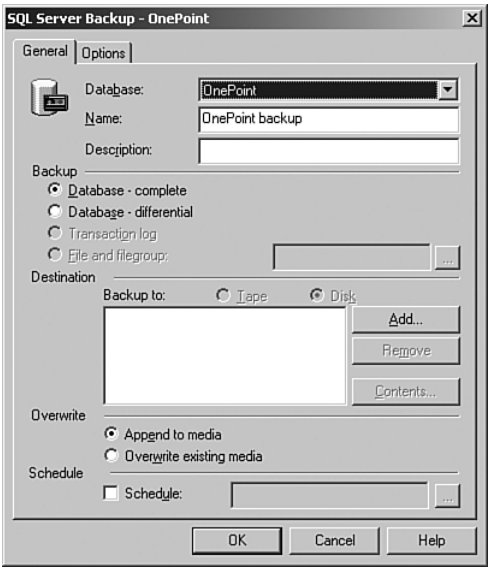


FIGURE 12.3 The SQL Server Enterprise Manager Backup screen.

2. The default backup type is Database - Complete, which is the backup type we want to use for the OnePoint database. Under Destination, select the backup destination, which can be a disk file or offline media such as tape. Here we will back up the OnePoint database to disk.

3. Select Add under Destination. The wizard provides a default location of *%ProgramFiles%*\Microsoft SQL Server\MSSQL\Backup. To enter the filename where the backup will be stored, click on the button with the ellipses (…).

   We will name our file OnePoint_Full_Group1.bak. Figure 12.4 shows the location specified for the backup file.

Backup Naming Conventions

Because you may have more than one management group, you may want to include the management group name as part of the filename for your backup files. You may also want to include the type of backup, so that a name for the MOM database backup might be OnePoint_Full_<*management group name*>.bak.

4. After specifying the filename and location, decide whether you will overwrite the file. By default, SQL Server appends the current backup to the end of the backup file if it already exists. You also have the option to overwrite (replace) the file. If your

nightly backup process includes backing up the file containing the OnePoint database backup to storage media, you can overwrite the disk file.

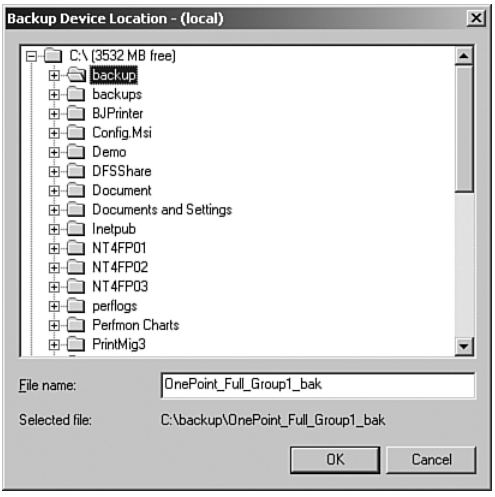


FIGURE 12.4 The backup device location screen.

5. Define a schedule for the OnePoint database backup. If you click the Schedule check box, SQL Server automatically creates a default schedule of weekly. The recommended backup frequency for the OnePoint database is nightly, so click on the ellipses (…) next to the schedule to proceed to the Schedule screen shown in Figure 12.5.

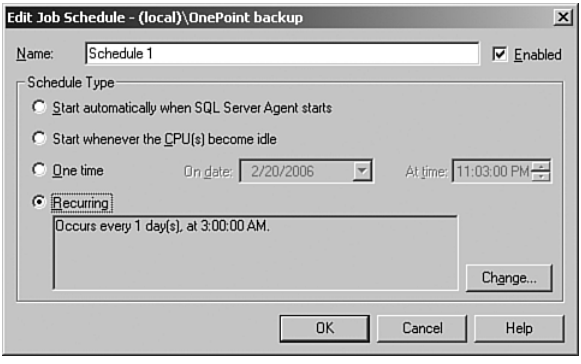


FIGURE 12.5 The Edit Job Schedule screen.

6. Click the Change button to change the schedule from weekly to daily. Figure 12.6 shows the updated Occurs value changed to daily and the start time at 3:00 AM rather than the 12:00 AM default start time.

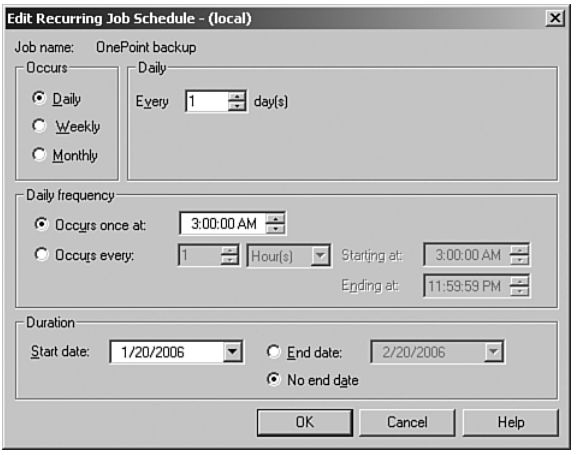


FIGURE 12.6 The Edit Recurring Job Schedule screen.

Scheduling Database Backups

Set the start time for a time where the backup does not interfere with the nightly groom job (which starts at 12:00 a.m.) and the nightly Data Transformation Services (DTS) job if you have MOM Reporting installed, which by default runs at 1:00 a.m. To avoid contention, give the DTS job time to complete before starting the OnePoint backup.

SQL Server backup operations can occur while the database is online and in use.

After defining the database backup, make sure that there are procedures in place to copy the file you create from the OnePoint database backup to back up media. You can use your existing nightly file backup process, adding the OnePoint backup file to the list of files and folders being backed up. In addition, you should make sure that the other files mentioned earlier—.akm and .xml files, the ManualMC.txt, custom .omc files, custom .msc files, and the file transfer service files—are also backed up regularly as part of your daily backup procedure.

More on Database Maintenance and Backups

Besides the fairly obvious reason for doing backups mentioned earlier—that of having a database to restore in the event of damage to the database or disk—another reason is to keep the size of the transaction log manageable, which keeps MOM functional.

What is a transaction log? All updates to a SQL Server database are first written to its transaction log. The transaction log exists because SQL Server supports transaction processing. A *transaction* is a logical unit of work—all operations defined as a transaction will either succeed or fail together. For example, assume you want to move $500 from your checking account to your savings account. If the money is removed from your checking account but never deposited into savings, you have lost $500—it just disappeared! Transaction processing allows these two operations to be grouped into a

single transaction, maintaining data integrity. If your deposit doesn't get to your savings account, the transaction is not "committed"—it is incomplete, and the update to your checking account is "rolled back"—and the $500 is still in your checking account.

The transaction log keeps track of every data modification performed in your database, who performed it, and when. However, if records are not eventually deleted from the transaction log, the file will fill up—or if autogrow is enabled—grow until it fills all available space on the disk(s) holding the physical log files. SQL Server automatically truncates the log every time a checkpoint is processed, which occurs by executing a `CHECKPOINT` statement, modifying the database using the `ALTER` command or the graphical database tool, or shutting down the SQL Server instance.

Because OnePoint (and SystemCenterReporting) uses a simple recovery model—which does not utilize the transaction log during database restores—all log records other than those at the active portion of the log can be truncated at any time, unless you are running a database backup. To initiate the truncate operation, you would run the following SQL statement:

```
BACKUP LOG OnePoint WITH TRUNCATE_ONLY
```

You could add this statement as a job step to the backup job you create for the database segment. In SQL Server Enterprise Manager, navigate to your database server, select Management, and then select Jobs, edit the Backup job, and add a second step with the options shown in Figure 12.7.

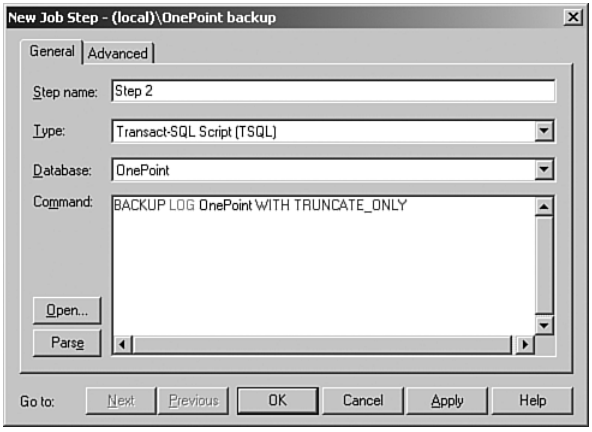


FIGURE 12.7 Truncate the transaction log during the backup process.

You would have to add this step manually; you cannot use Enterprise Manager (or SQL Server Management Studio) to configure a transaction log backup when the database is configured for simple recovery.

For databases that use the simple recovery model SQL Server generates an automatic checkpoint—which deletes the inactive portion of the log—when the log becomes 70% full. You can see why autogrow would not be a good idea here—the log will never

become 70% full if it can always grow! You can also set a checkpoint yourself to delete the inactive portion of the log using the following syntax:

```
USE OnePoint
CHECKPOINT
```

If your log should fill up, don't panic. Run the following statement to remove the inactive portion of the log and not log the operation:

```
DUMP TRANSACTION OnePoint WITH NO_LOG
```

These commands can also be run against the SystemCenterReporting database.

Database Restores

If one of the MOM databases becomes corrupt or a hardware issue causes you to lose a database, you will need to restore the affected database(s). We will build on the previous example where we created a backup of the OnePoint database using Enterprise Manager. For our scenario, we will assume that the OnePoint database is corrupt and cannot be repaired. At this point, our strategy is to restore from the latest backup.

1. To ensure that MOM does not try to write data to the OnePoint database during the restore process, stop the MOM service on the management server. This prevents agents from sending data to the management server. Stopping the MOM service also prevents MOM from trying to write data to the OnePoint database.

Role of MOM Queue Files

Remember that data is stored in queue files when the OnePoint database is unavailable, which minimizes the chance of data loss.

2. Before performing a full restore for a SQL Server database, you must take the existing instance offline. Launch SQL Enterprise Manager and navigate to Microsoft SQL Servers \ SQL Server Group \ Local \ Databases \ OnePoint. Right-click on OnePoint, select All Tasks, and select Take Offline, as displayed in Figure 12.8.
3. Restore the database from the last backup. Right-click on Databases and select All Tasks/Restore Database. This displays the Restore Database screen shown in Figure 12.9.
4. Enter **OnePoint** in the Restore as Database text box. Under Parameters you are given a drop-down list for Show Backups of Database. Select OnePoint to display the backup history for the database. Verify that the latest backup is selected for restore and click OK to begin the restore process. Depending on the size of your database, this may take several minutes.

After you restore the database, restart the MOM service and launch the MOM Administrator console to verify it has the correct rule groups and configuration. You can

also launch the MOM Operator console to make sure that agents are sending heartbeats. This ensures that MOM is operational.

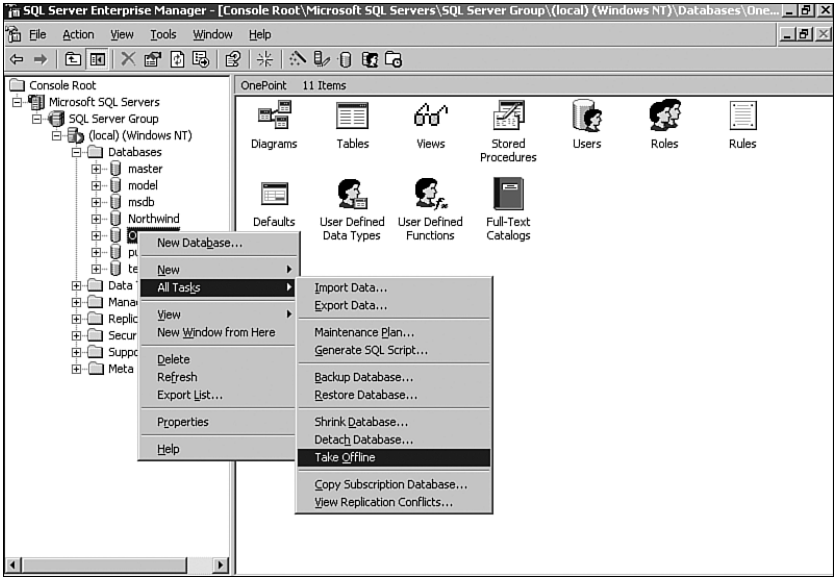


FIGURE 12.8 Take the database offline.

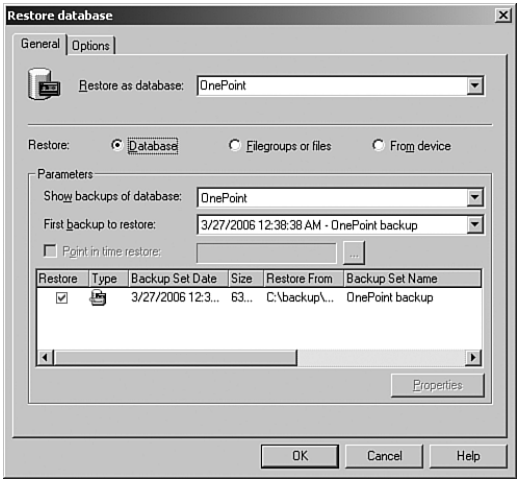


FIGURE 12.9 The Restore Database screen.

Restoring Databases Used by MOM

When restoring the OnePoint or the SystemCenterReporting databases be sure the MOM or SQL Server Reporting Services (SSRS) software installed is at the corresponding service level of your database backup. As an example, you cannot install SSRS without a service pack and then use a SystemCenterReporting database that has Service Pack 1 or Service Pack 2 applied to it.

The installation is blocked if you try to install without matching levels of maintenance.

SQL Server 2005 Backup and Restore Steps

The following procedure defines a backup job for the SQL Server 2005 OnePoint database:

1. In SQL Server Management Studio, navigate to Microsoft SQL Servers \ SQL Server Group \ Local \ Databases \ OnePoint. Right-click on the OnePoint database, select Tasks, and then choose Backup, which brings up the Back Up Database General page shown in Figure 12.10.

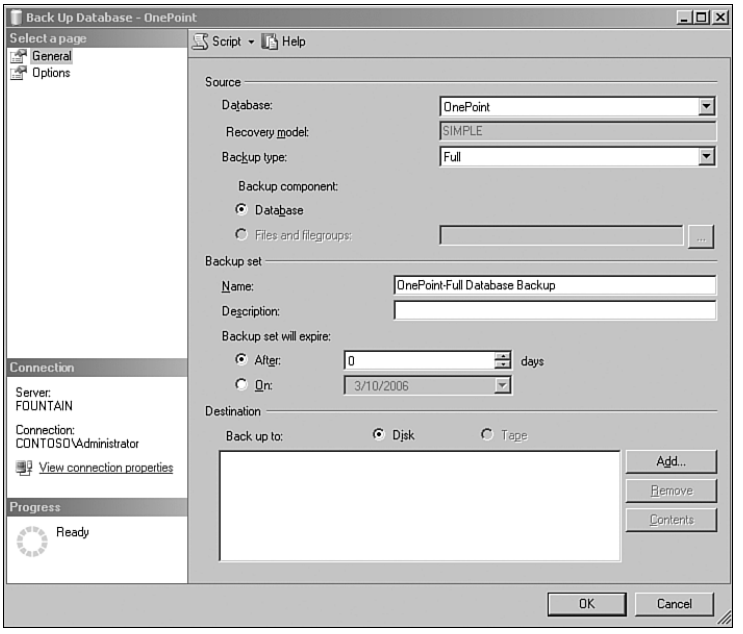


FIGURE 12.10 The SQL Server Management Studio Manager backup screen.

2. The default backup type is Full, which is the backup type we will use for the OnePoint database. Under Destination, select the backup destination, which can be a disk file or tape. Here we will back up the OnePoint database to disk, which is the default.

3. Select Add under Destination. The wizard provides a default location of *%ProgramFiles%*\Microsoft SQL Server\MSSQL\Backup. To enter the location and filename where the backup will be stored, click on the button with the ellipses (...) and name the file OnePoint_Full_Group1.bak. Figure 12.11 shows the location specified for the backup file.

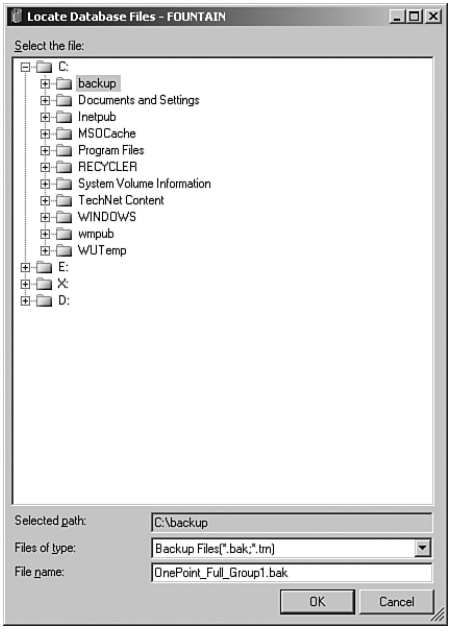


FIGURE 12.11 The backup device location screen.

4. SQL Server Management Studio next displays the Select Backup Destination screen, shown in Figure 12.12.

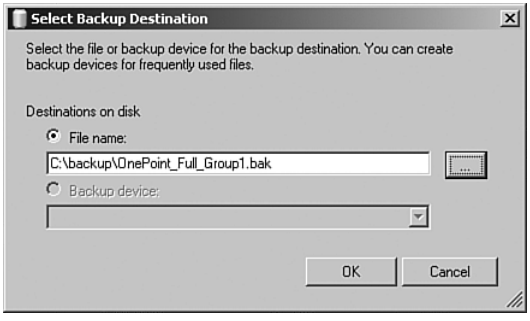


FIGURE 12.12 The Select Backup Destination screen.

5. After specifying the general requirements for the backup, it is time to move to the Options page shown in Figure 12.13. You must decide whether you will overwrite the file (backup set). By default, SQL Server appends the current backup to the end of the backup file if it already exists. Alternatively, you can overwrite (replace) the file. The option to truncate the transaction log is grayed out because SQL Management Studio will not let us truncate the log when the database recovery type is defined as simple. We will have to add a step to truncate the log manually.

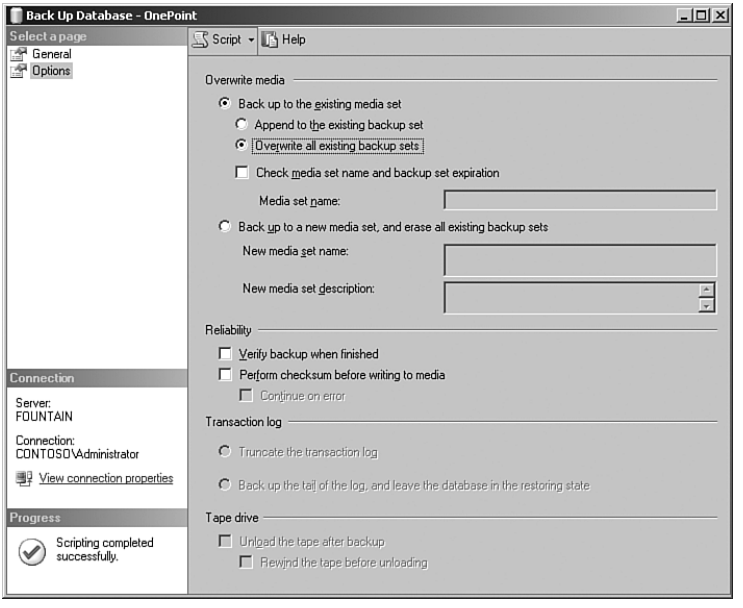


FIGURE 12.13 The backup options page.

6. Selecting the Script option at the top of Figure 12.13 generates Transact SQL code you can use to schedule the backup rather than having to return to SQL Management Studio each time you want to back up the database. (After the script is generated, the progress shows that scripting completed successfully.)
7. After generating the script, select the Script menu at the top of the panel to bring up scripting options. You can direct the script action to a query window, save it to a file, copy it to the Clipboard, or schedule it as a job. We want to schedule the backup as a SQL job, so we will select the Script Action to Job option, which is displayed in Figure 12.14.
8. Define the parameters of the backup job. When we selected the Script Action to Job option, it opens the New Job dialog. At the General page, we can change the owner and category of our job. In this case we will take the defaults shown in Figure 12.15.

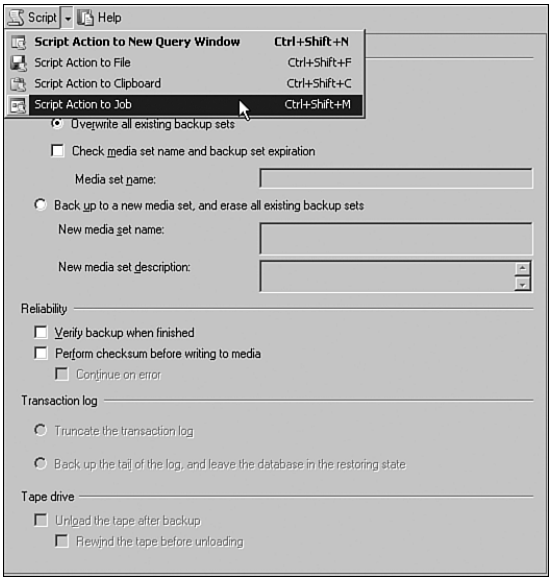


FIGURE 12.14 Create a SQL backup job.

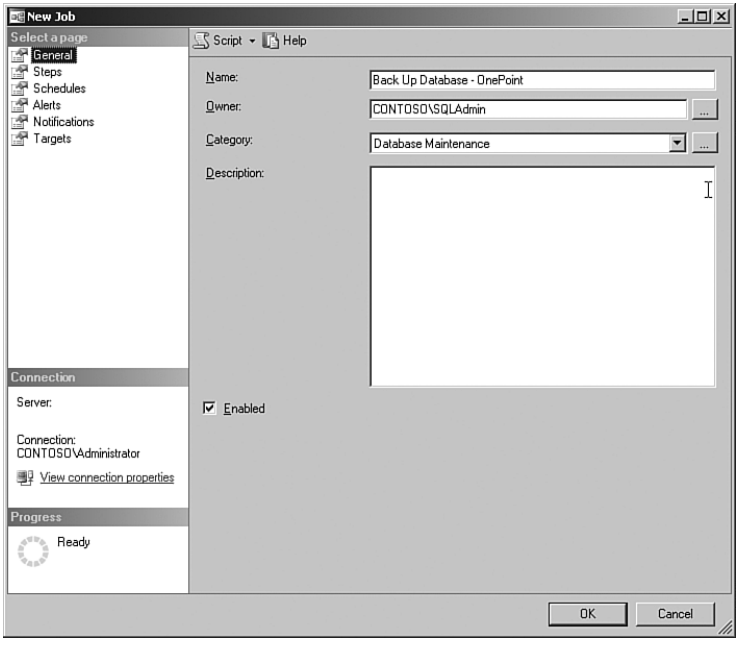


FIGURE 12.15 The new job screen.

9. Select the Schedules page (see Figure 12.16) and click New to add a new schedule.

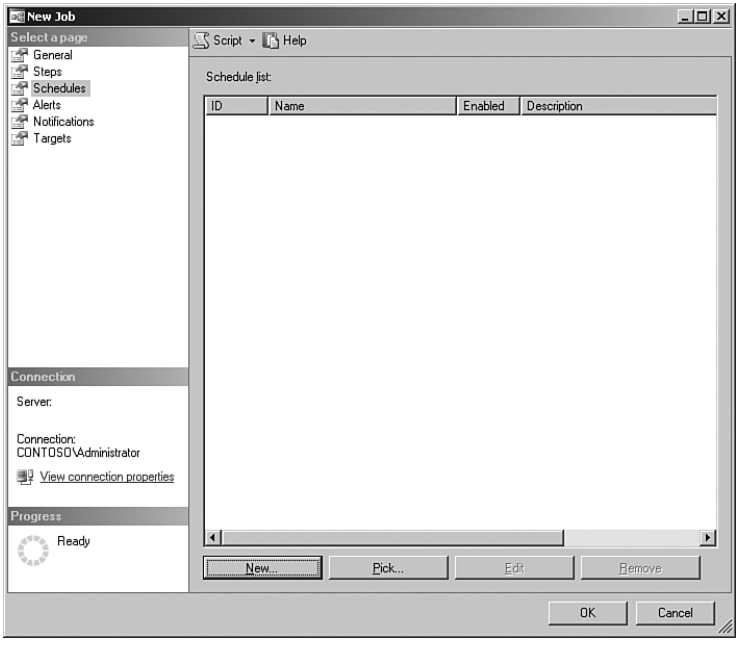


FIGURE 12.16 The New Job Schedules page.

10. You can now define the details of the schedule. In Figure 12.17 we have scheduled a type of Recurring with a backup frequency of daily and a start time of 3:00 AM. After completing this screen, you can also specify Notifications and Targets as part of the job properties. Click OK to save the job.

After creating the database backup step, you will also want to truncate the transaction log. Truncating the transaction log has to be defined manually because the MOM database uses the simple recovery model. The following SQL statement initiates the truncate operation:

```
BACKUP LOG OnePoint WITH TRUNCATE_ONLY
```

You can add this statement as a job step to the backup job you just created for the database segment. In SQL Server Management Studio, navigate to your database server, select Management, select Jobs, and then edit the OnePoint backup job and add a second step with the options shown in Figure 12.18.

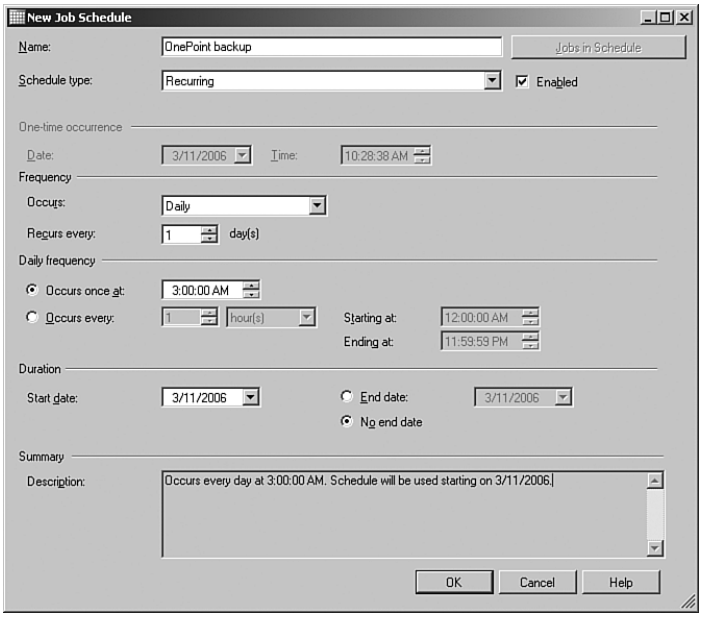


FIGURE 12.17 The recurring job schedule screen.

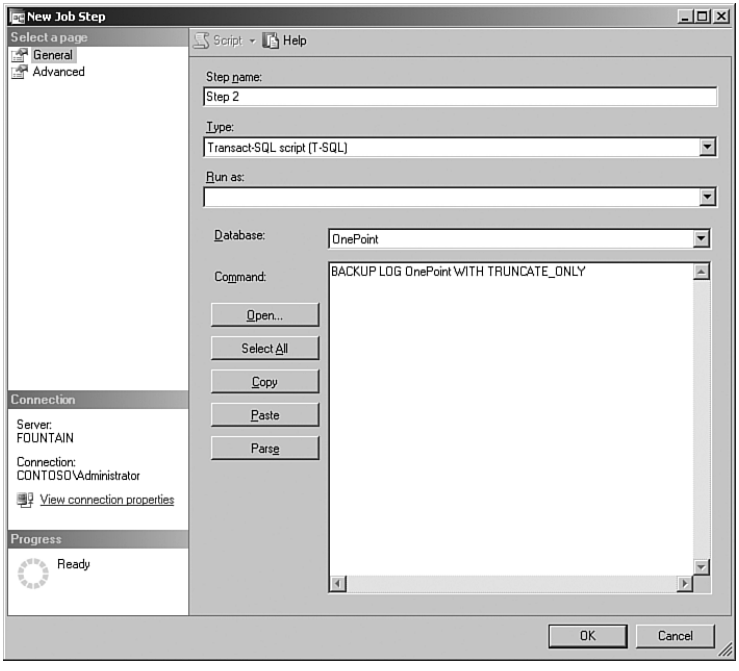


FIGURE 12.18 Truncate the transaction log as part of the backup process.

The following procedure discusses the process of restoring the OnePoint database:

To restore the OnePoint database, you will want to use the latest backup. Be sure to stop the MOM service on the management server to ensure that MOM will not try to write data to the database.

1. Before performing a full restore for a SQL Server database, you must delete the existing version of the database. Launch SQL Server Management Studio and navigate to Microsoft SQL Servers \ SQL Server Group \ Local \ Databases \ OnePoint. Right-click on OnePoint and select Delete. Uncheck the option to delete backup and restore history information from the database; then click OK to delete the OnePoint database.
2. Restore the database from the last backup. Right-click on Databases and select Restore Database. In the Source for Restore section, select From Database, and select OnePoint from the drop-down list. This displays the Restore Database screen as shown in Figure 12.19.

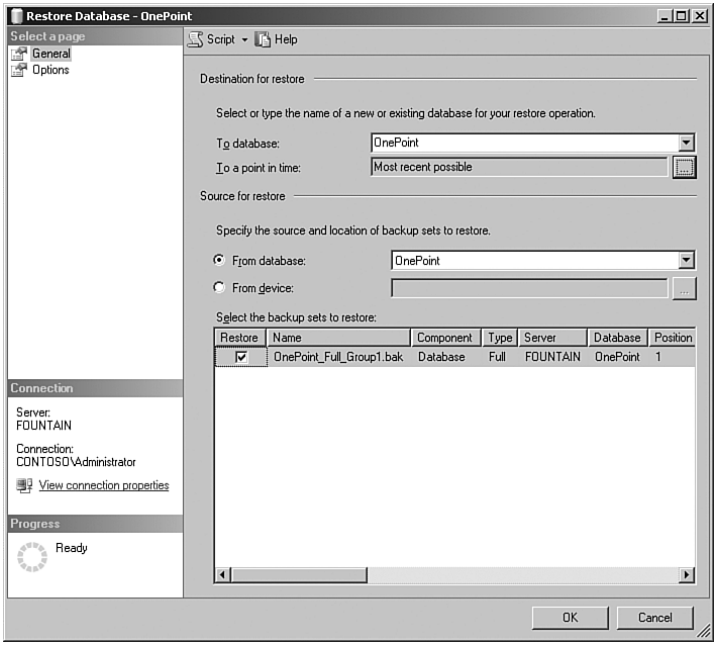


FIGURE 12.19 The restore database screen.

3. If there is more than one backup, verify that the latest one is selected for restore and click OK to begin the restore process.

Backing Up Management Packs

Management packs, which reside in the OnePoint database, should be backed up separately in addition to your regular database backups. Having management pack backups

enables you to quickly restore rules that may have been accidentally modified and is also necessary to restore custom rules if you use the MOM-to-MOM Product Connector in a multitiered MOM configuration. Backing up a management pack after making changes to it gives you the granularity to restore just that management pack.

Management packs can be backed up either with the Administrator console or a command-line utility.

Using the MOM Administrator Console

Chapter 13, "Administering Management Packs," fully describes using the Administrator console to export and import management packs. The functionality can also be used as part of your backup strategy. In this chapter we will focus on those steps of particular significance when backing up management packs.

To use the MOM Administrator console to back up and restore management packs, perform the following steps:

1. Right-click on the Management Pack icon on the Navigation pane in the Administrator console and select Import/Export Management Pack to launch the Import/Export Management Pack Wizard, shown in Figure 12.20.

FIGURE 12.20 Welcome to the Management Pack Import/Export Wizard.

2. We will back up the management pack, so it is necessary to select Export Management Packs and continue.

3. At the Select Rule Group dialog you can drill down to the management pack you want to back up. We will back up the PingPack management pack discussed in Chapter 20, "Developing Management Packs." Figure 12.21 shows the PingPack rule group selected for backup.

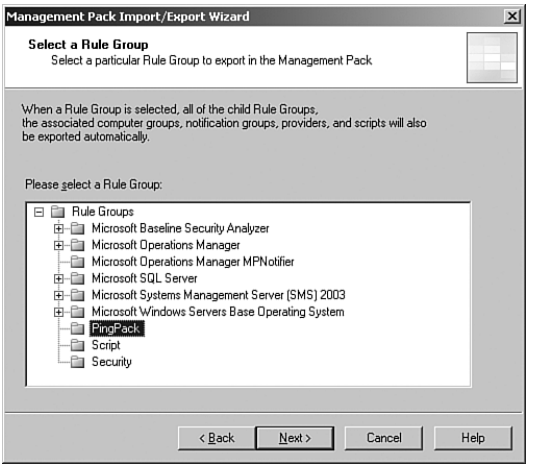


FIGURE 12.21 The Select a Rule Group screen in the Import/Export Wizard.

4. The next screens ask whether you want to export existing views and tasks associated with the management pack. Because you want to back up the entire management pack, you would select all applicable views and tasks here. In this particular case, the PingPack management pack does not include views, so click Next to advance to the Select Tasks screen, where you can expand the selection by clicking on the "+" icon. Select the checkbox next to PingPack to specify all PingPack tasks, and Click Next.

5. You are asked to specify the name of the export file. Management pack files are stored in the file system with an extension of .akm. Figure 12.22 shows that we will export the PingPack management pack in a file named C:\Management Packs\PingPack.akm.

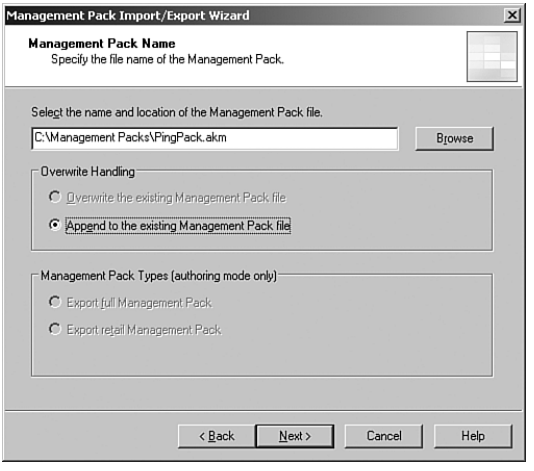


FIGURE 12.22 Naming the exported management pack.

6. You can append to the file if it exists, or overwrite it. Overwriting the file overlays any previous exports written to that file. Finally, the wizard displays a summary of the options you specified, and the export is initiated after you click Finish. You will see an Export Status screen that ultimately tells you whether the export (backup) was successful.

Restoring the management pack using the MOM Administrator console is accomplished using the Import function discussed in Chapter 13.

Using the ManagementModuleUtil.exe Command-Line Utility

Another way to backup and restore management packs is with a command-line utility that ships with MOM 2005 called ManagementModuleUtil.exe. There are several advantages to using this utility versus the MOM Administrator console:

- If you have a number of management packs to back up, you can create a batch file containing commands for each management pack.
- Commands can be scheduled as batch jobs using Task Scheduler or the AT command for automated daily backups of the management packs.
- You can synchronize rule groups across management groups when you have multi-tiered MOM environments. You can use batch files run by the Scheduler to export from a child management group to a parent group, or from pilot to production networks.

The ManagementModuleUtil.exe utility resides in the *%ProgramFiles%*\Microsoft Operations Manager 2005 folder. You can view the syntax for the utility by typing **managementmoduleutil.exe** from a command prompt (assuming that your path includes *%ProgramFiles%*\Microsoft Operations Manager 2005; otherwise, navigate to this directory).

Exporting Management Packs

The syntax to export a management pack is

```
ManagementModuleUtil.exe -O MOMServerName MPObjectName AKMFileName -W
```

Table 12.3 describes the export parameters for ManagementModuleUtil.

TABLE 12.3 `ManagementModuleUtil` Options to Export a Management Pack

Parameter	Description
`-O`	Performs a complete export of a rule group
`-Ox`	Performs a complete export of a rule group into retail format. In a retail version, the knowledge base is read-only, and any rules marked for deletion are dropped.
`-Ov`	Performs an export of a saved view.
`-Ot`	Performs an export of a task.

TABLE 12.3 `ManagementModuleUtil` Options to Export a Management Pack

Parameter	Description
`MOMServerName`	Name of the management server.
`MPObjectName`	Name of the MOM object (management pack in this instance) being exported. If the name of the object is multiple words, enclose the name in double quotes (example: "Microsoft Operations Manager").
`AKMFileName`	Filename that the management pack is being exported to (enclose in double-quotation marks if it contains spaces).
`-W`	Writes to a new .akm file.
`-A`	Appends to an existing .akm file.

To continue with our previous example where we backed up our PingPack management pack with the Administrator console, you would use the following command to export it using ManagementModuleUtil.exe:

```
ManagementModuleUtil.exe -O monarch PingPack "C:\Management Packs\PingPack.akm" -W
```

In this example Monarch is the name of our management server. Note that the name of the management pack (PingPack) is case sensitive when using ManagementModuleUtil.exe.

Importing Management Packs

To import a management pack into a management server using ManagementModuleUtil, use the following procedure:

1. At the command line, go to the %*ProgramFiles*%\Microsoft Operations Manager 2005 directory.
2. Execute the batch utility by using the syntax

   ```
   ManagementModuleUtil.exe -I MOMServerName AKMFileName [-R][-V]
   ```

Update is the default Import option and is used if you do not specify `-R` (Replace) or `-F` (Force). Table 12.4 lists the parameters used for importing a rule group with this utility.

TABLE 12.4 `ManagementModuleUtil` Options to Import a Management Pack

Parameter	Description
`-I`	Imports a rule group.
`MOMServerName`	Name of the management server.
`AKMFileName`	Filename that the management pack is being imported from (enclose in double-quotation marks if it contains spaces).
`-R`	Replaces the entire rule group; all customizations of existing management pack objects are overwritten.

TABLE 12.4 Continued

Parameter	Description
-F	Forces the existing management pack objects to be merged with the ones in the AKM file. Customer Knowledge is retained, the enable/disable setting is retained, and customer rules are retained. All other information is overwritten. Although this functionality remains within ManagementModuleUtil, it is for backward compatibility with MOM 2000 only and is no longer recommended by Microsoft.
-V	Disable Import Version Verification.

To import the PingPack management pack, you would use the following command line:

```
ManagementModuleUtil.exe -I monarch "C:\Management Packs\PingPack.akm" -R
```

The -R option replaces the current management pack with the management pack backup. Alternatively, you could use the -F flag to merge the current with the backup. If neither the -F or -R flag is specified, the default is that the imported rules are merged with the existing rules, and rule changes are kept.

Information on ManagementModuleUtil

The ManagementModuleUtil utility is also distributed with the MOM 2005 SDK. Full documentation on this tool is available on the Microsoft MSDN website at http://go.microsoft.com/fwlink/?LinkId=50273.

Backing Up Reports

ManagementModuleUtil does not backup reports. The equivalent command-line utility for exporting and importing reports you have developed yourself is the RptUtil.exe utility.

RptUtil is installed as part of SSRS and can be found on the computer where you installed MOM Reporting at *%ProgramFiles%*\Microsoft System Center\Reporting\RptUtil.exe. RptUtil was designed to export and import SRSS reports. We recommend that you export at the folder level rather than individual reports. Reports are exported to the file system as XML files. Table 12.5 lists the parameters used by RptUtil.

TABLE 12.5 RptUtil Parameters

Parameter	Description
/action:export	Action—import or export (Default=export)
/file:	Full path to the import or export file. (Default=C:\MOMReports.XML)
/url:	URL of the report server. URL can end with or without ReportService.asmx. Default=http://localhost/ReportServer/ReportService.asmx)

TABLE 12.5 Continued

Parameter	Description
`/reportpath:`	Path to the report or report folder to be exported. Valid only when action=export (Default=/)
`/fromdsref:`	Name of the "from" data source reference to fix up. Valid only when action=import (Default=SCDW)
`/todsref`	Name of the "to" data source reference to fix up. Valid only when action=import (Default=/SCDW)
`/datasource:`	Name of the datasource to fix up. Valid only when action=import (Default=SCDW)
`/dwserver:`	Name of the data warehouse server used to fix up the data source. Valid only when action=import (Default=.)
`/dwdb`	Name of the data warehouse database used to fix up the data source. Valid only when action=import (Default=SystemCenterReporting)
`/nowarn`	Do not warn if reporting server is not configured to use SSL.
`/noprompt`	Do not prompt for user input. Use this option when running an automated script. (Default is to prompt if needed.)

Using the default locations, the syntax to export a report from the command line would be:

```
RptUtil /action:export /file:C:\MOMReports.XML /url:http://localhost/ReportServer
/reportpath:/
```

For example, let's say that you have created a number of reports to graph growth of the MOM databases. You would use the following procedure to export all reports within the MOM Database Tracking report folder to a file named MOM Database Tracking.xml on the root of the E: drive:

1. At the command prompt, change to %*ProgramFiles*%\Microsoft System Center Reporting\Reporting. (If you installed System Center to the C: drive, you would change to C:\Program Files\Microsoft System Center Reporting\Reporting.)
2. Execute the following RptUtil command:

   ```
   RptUtil /action:export /file:"E:\MOM Database Tracking.xml"
   /url:http://localhost/ReportServer /reportpath:"/Microsoft Operations Manager
   Reporting/MOM Database Tracking"
   ```

3. If you receive an SSL warning, press Enter to continue.
4. Verify that the XML file has been created.

You can use the import function of the Management Pack Import/Export Wizard (discussed in Chapter 13) or RptUtil to load any customized reports back into the ReportServer database. RptUtil syntax to import the MOM Database Tracking reports just exported would be

```
RptUtil /action:import /file:"E:\MOM Database Tracking.xml" /nowarn
```

Backing Up SQL Reporting Services Encryption Keys

The SQL Server Reporting Services setup process creates encryption keys that are used to secure credentials, connection information, and accounts used with server operations. If you should need to rebuild or repair your SSRS installation, you must apply the key to make the report server database operational. If the key cannot be restored, database recovery will require deleting the encrypted data and respecifying any values that require encryption.

The RSKeyMgmt.exe utility can be used to extract a copy of the encryption key from the ReportServer database. The utility writes the key to a file you specify and scrambles that key using a password you provide. This file should be backed up as part of your backup and recovery procedures. You should also document the password used for the file. Table 12.6 lists the parameters used by RSKeyMgmt.

TABLE 12.6 RSKeyMgmt Parameters

Parameter	Value	Description
`-e`		Extract a key from a report server instance
`-a`		Apply a key to a report server instance
`-d`		Delete all encrypted content from a report server database
`-r`	installationID	Remove the key for the specified installation ID
`-f`	file	Full path and filename to read/write key
`-p`	password	Password used to encrypt or decrypt key
`-t`		Include trace information in error message

To create a backup of the encryption key, use the following syntax:

```
RSKeyMgmt -e -fC:\rsdbkey.txt -p<password>
```

You would run this locally on the computer hosting the report server. Managing the encryption keys is discussed in the SQL Server Reporting Services Books Online under "Managing Encryption Keys." Michael Pearson has written an excellent article discussing SSRS Recovery Planning, available online from the SQL Server Central community (SQLServerCentral.com) at http://www.sqlservercentral.com/columnists/mpearson/recoveryplanningforsqlreportingservices.asp.

Automating the Backup Process

As an aid to backing up the files discussed in this chapter, we have created a simple batch file that automates the process from the command line. The backup scripts in the batch file are intended as an example and can be customized for your own environment. The database backup syntax is compatible with both SQL Server 2000 and SQL Server 2005.

The batch file (backup.bat) and a management pack (Scheduled Backup.akm) that runs the batch file are on the CD included with this book.

The management pack contains a single rule scheduled to run as a timed event nightly at 11:10 p.m., executing the batch file at c:\backup\backup.bat. Customize the associated Scheduled Backup computer group to include the servers with components you are backing up. For example, if all MOM components are on a single server, the computer group contains only that server. If your management server, database server, and reporting server are on separate computers, add each server to the computer group and customize the batch file on that system for the appropriate roles.

Chapter 13 discusses the structure of management packs including rules and computer groups.

Disaster Recovery Planning

Although we hope you never need to restore MOM from a catastrophic failure, you must be prepared for the possibility that this could happen. You should have a well-documented recovery plan that would work for every conceivable type of disaster that could occur, from hardware failures to a total datacenter loss. Essentially, you want to be able to get MOM up and running with minimal data loss.

Your plan should assume the worst but be able to concisely and efficiently restore MOM at a minimum to the last backup of the OnePoint database. Let's discuss what it would take to recover MOM assuming a "total loss." We will assume the following scenario:

- The OnePoint database is installed on the management server.
- The management server is monitoring 200 agent-managed systems.
- There is only one MOM management server in our management group.
- The Web console is installed.
- MOM Reporting is not installed.

Although this is a simple implementation of Operations Manager, it is intended to show you the steps necessary to recover MOM from a complete hardware failure of the management server. We will assume that our server team has already built a new server using the same NetBIOS name in the same domain, installed SQL Server, and enabled IIS because we will use the MOM 2005 Web console. The appropriate level of service packs and security patches are applied—be sure to be at the same level of software maintenance that you had with your original system. We are ready to recover MOM.

At a general level, here are the steps involved:

1. Install MOM from the MOM 2005 installation media—selecting the option for a typical installation and using the same management group name as the original install. Remember that the group name is case sensitive. Specify the same accounts (DAS account, Management Server Action account) as used by your original installation.

This type of information should be documented as part of your disaster recovery planning. Detailed steps on installing MOM can be found in Chapter 6, "Installing MOM 2005."

2. After MOM is installed, immediately stop the MOM service to prevent existing agents from sending data to the server.
3. Install any additional MOM hotfixes previously installed with your original installation.
4. Delete the OnePoint database created from your MOM installation in step 1.
5. Restore the latest OnePoint database created from your SQL backup.
6. Restore any backed up custom files, such as the ManualMC.txt, custom .msc and .omc files, and file transfer service files.
7. Import any additional management packs that were loaded to your old management server or changed and backed up after your last OnePoint database backup.
8. Install the Web console.
9. Start the MOM service. The agents will now begin communicating with the server.

These steps constitute a high-level process for recovering MOM. Your actual plan should contain greater detail, including specific hard drive configurations, the exact installation options, the SQL steps necessary to delete and restore the OnePoint database, and so on. You need to not only develop a detailed plan but should also practice it in a development environment until you (and others on your staff for when you are not available) are comfortable with the process.

Summary

This chapter discussed the need for backups, the components to be backed up regularly, and the tools available for performing backups. We also discussed an approach for backing up the reporting database and overall disaster recovery planning for MOM. The next chapter covers administering management packs, including best practices for implementing management packs and Microsoft resources to help with management pack administration.

This page intentionally left blank

CHAPTER 13

Administering Management Packs

IN THIS CHAPTER

- Management Packs Defined
- Management Pack Information at Microsoft.com
- Management Pack Versions
- Planning for Deployment
- Managing Management Packs

This chapter discusses underlying concepts and fundamental uses of management packs. We step through the process of importing and exporting management packs, and discuss best practices for incorporating management packs into your MOM environment. We also discuss a number of utilities and resources developed by Microsoft to simplify management pack administration.

Any discussion of management packs invariably leads to questions about the alerts generated by those management packs. To that end we include a brief discussion of some tuning and troubleshooting techniques that can help in the proper implementation of management packs.

Management Packs Defined

Management packs (MPs) provide a snapshot of product and component health and are the mechanism MOM 2005 uses to manage and monitor specific applications and services. Management packs make it possible to collect and utilize a wide range of information from various sources. They describe what data to examine and provide analysis of that data.

Management packs are authored by Microsoft or by third parties. You may decide to write rules to augment or improve an existing MP or you might decide to create a management pack from scratch, particularly to manage a product where Microsoft or a third party has not released a corresponding management pack. In Chapter 20, "Developing Management Packs," we step through the process of developing management packs.

Management packs include collections of rule groups, rules, knowledge, computer attributes, computer groups, and public views; these components are used to determine how a management server collects, handles, and responds to data related to a specific monitored application or service. Management packs may also include scripts, tasks, or reports.

One of the strengths of MOM is that its management packs are typically produced by the same engineers who wrote the particular application or service. For instance, the management packs for Microsoft products are produced by the respective product teams. The management packs represent the best efforts of the developers to expose relevant and useful monitoring related information, to determine what issues require attention, and to assess the level of product knowledge required for administrators to resolve a given situation.

Rules Overview

Rules are a key component of management packs. Rules can be defined to detect the occurrence or absence of a certain condition or state, such as a scheduled backup completing successfully, or whether a performance count has exceeded a predefined threshold, such as requests backing up in a processing queue. Rules can also be defined to run a series of scripts performing synthetic transactions to verify such things as mail server response times and availabilities. Scripts can also collect information to be used for state monitoring and reports.

A rule generates an alert when it determines that something worthy of attention has occurred. The alert requires an administrator's intervention to address a potential outage or look at issues that may affect server performance and availability. Alerts are coupled with Knowledge articles, which give a summary of the issue and its impact, list potential causes, and provide resolution steps to address the issue itself. This information enables technicians to quickly address detected problems. The knowledge often enables first-level operators and support personnel to address a number of issues on their own, facilitating a faster turnaround and fewer escalations.

Rules can be used for a variety of functions, including

- Identifying performance data, events, and other types of information to be collected from managed computers
- Defining how collected data should be processed
- Filtering out duplicate or unimportant data
- Specifying responses when the data evaluated indicate a certain condition or state. Responses can include generating an alert, executing a script or command, updating a state variable, notification by email or pager, or transferring a file. Rules that generate alerts can also be configured to set state.

Configuring Email Notification

If you are using email notifications as responses, you may need to modify the registry to send Simple Mail Transfer Protocol (SMTP) email. KB article 885741 (http://support.microsoft.com/kb/885741/) discusses error 2147220975 and how to properly configure the SMTP server.

There are three types of rules:

- *Event rules* include alerts, responses to events, collection rules, filtering rules, detecting missing event rules, and consolidation rules.
- *Performance rules* consist of measuring rules and threshold rules.

  Measuring rules cause MOM to collect numeric values from sources such as WMI or Windows performance counters. MOM stores sampled numeric measures in its database.

  Threshold rules specify that MOM generate an alert or execute a response when a WMI value or performance counter crosses a defined threshold.
- *Alert rules* define responses to be taken when an alert has been generated by another rule.

A rule is primarily made up of a data provider, criteria, a response, and knowledge pertaining to that rule. Figure 13.1 illustrates the key parts of a rule.

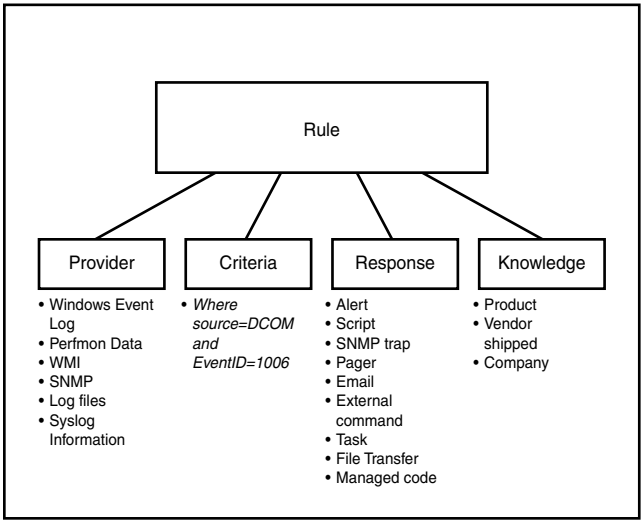


FIGURE 13.1 Rule components.

Chapter 14, "Monitoring with MOM," covers rule types and components in detail.

Other Components

In addition to rules, the following components may be contained in a management pack:

- *Rule groups* are sets of rules that enable organization of rules in a logical structure. Rule groups also enable deploying rules through an association with a computer group. Rule groups can be nested, such that the Microsoft Windows Servers Base Operating System rule group contains the Windows (All Versions), Windows 2000, Windows 2003, and Windows NT 4.0 rule groups. Each of these rule groups also has rule groups defined within them as well, so a hierarchy can be multileveled. A typical structure for a rule group would be as follows:

```
%Product Application Name%
    %Product Application Version%
        %Component%
            %Sub Component%
```

  When a rule group is associated with a computer group, the rules within the rule group and any child rule groups are deployed to members of the computer group.

- *Data providers* tell rules where to look on managed computers for relevant information utilized by MOM. Providers include Windows Operating System event logs, performance counters, SNMP data, WMI information, timed event providers, application log files, and syslogs. Custom data providers can also be created.

- *Scripts* can be added to a rule as a response and can also be used to extend the capabilities or rules. Scripts can be written using Microsoft Visual Basic Script Edition (VBScript) or Microsoft JScript. You can also specify a language choice of Custom; this can be any custom active scripting language such as Perl, although the custom scripting engine must be installed on all computers where the script will run. Scripts can be designed to perform many functions and can create additional events and performance data that may be evaluated by other rules.

- *Computer attributes* are used as part of a computer group's formula and enable groupings of computers with common computer attributes. These attributes reference values or keys found in the registry, which are then collected across the enterprise via MOM's attribute discovery process.

  For example, the formula for determining the membership for the computer group Microsoft Windows Servers is `AttributeValue(Microsoft Windows Current Version)>="4.0"`. If a managed computer attribute matches these values, the computer is made a member of the group. You can also manually include or exclude a computer in a computer group by name and domain.

  The membership formula can get complicated as can be seen in the formula for the Microsoft Exchange Server 2003 Backend computer group:

```
(AttributeValue(MSExchange Server) AND AttributeValue(MSExchange Server
Version) = 6944) AND (AttributeValue(ExchangeService) = "Exchange 2003") AND
(NOT (AttributeValue(Virtual Server Type) OR AttributeValue(IsHostingMSCS)) OR
```

```
(MatchRegEx(AttributeValue(Virtual Server Type), "(^¦,)Microsoft[ ]Exchange[
]System[ ]Attendant($¦,)")))
```

Identifying Computer Membership in Computer Groups

You can use the Operator console to determine which computer groups a computer belongs to:

1. Select the Computers and Groups Views Navigation pane.
2. Select Computers; then select a particular computer within the Results pane.
3. In the Details pane click on the Computer Groups tab to see group membership.

Another approach, nowhere as elegant, is to write an SQL Server query. The SQL Server SDKComputerToComputerGroupView, documented in the Microsoft Operations Manager 2005 Software Development Kit (SDK), provides a way to list which computers belong to a specific computer group. A sample query might look like this:

```
Select ComputerGroupName, ComputerName from SDKComputerToComputerGroupView
where ComputerGroupName = 'Microsoft SQL Server 2005'
```

The query lists the SQL Server 2005 systems belonging to the Microsoft SQL Server 2005 computer group.

- *Computer groups* are collections of computers with similar characteristics or purposes. The collection is based on common attributes or uses a formula specified for the computer group. Computer groups serve many purposes, such as targeting rules, defining console scopes, and viewing selected computers in the MOM Operator and Reporting consoles. To deploy rules in a rule group to agents, the rule group must be associated with one or more computer groups.

Using Computer Groups to Associate Rules

A common approach used in management packs is associating rules with different computer groups based on whether the target system is an agent-managed or agentless computer. The SQL Server MP utilizes this approach using a computer group for agentless servers.

- *Notification groups* are used by notification responses within event, performance, and alert rules. Notification groups list operators that will be notified when a notification response is executed and are functionally similar to a distribution group or list.
- *Views* enable different representations in the Operator console of operational data that has been collected by a management pack. Views enable a user to view alerts, events, performance, state, attribute, and diagram information in various ways.
- *Diagrams* are a type of view displaying computers and their relationships in the Operator console. These diagrams are dynamic and discovered by the management packs. The Diagram view lets you see the status of each node in your topology, navigate to other views, and launch context-sensitive actions.

- *Tasks* are predefined commands or processes that can be useful for someone managing a particular application. Tasks can be used for diagnostics or to assist in resolving issues. Tasks can be executed from the Operator console or can be agent-targeted.
- *Service discovery* enables discovery of entities that will be managed and/or exposed in reports (such as an application configuration). Service discovery includes discovery of entities and their properties, as well as defining relationships with other entities.
- *Knowledge* associated with the rules specifies how problems should be corrected and how the management pack should be used. Knowledge summarizes the issue and can define the impact on the application, expose probable causes, and provide resolution steps.
- *Reports* are included as part of a management pack package in a separate XML file. MOM Reporting utilizes SQL Server Reporting Services to provide reports that are easily customizable using Visual Studio.NET. Using the Reporting console, you can view event, alert, and performance reports using a web browser. Reports can be exported to a variety of formats, including Microsoft Excel, Adobe Acrobat, HTML, TIFF, CSV, or XML file formats.

Management Pack Information at Microsoft.com

Microsoft has written management pack guides giving in-depth information and deployment details for many of the management packs for Microsoft products. The guides for Microsoft's management packs are available with the MOM 2005 Service Pack 1 (SP1) documentation at http://go.microsoft.com/fwlink/?linkid=49776. Guides are also often distributed within the download package for a particular management pack.

Microsoft's Management Pack and Utilities Catalog provide one-stop shopping for management packs from Microsoft and third-party vendors. The catalog is located at http://go.microsoft.com/fwlink/?linkid=43970 and provides a central location for accessing MOM management packs. The web page also includes links to the Operations Manager Connector and SMS Add-in catalogs.

Using the Management Pack Catalog and the Management Pack Notifier

The Management Pack Catalog site (http://go.microsoft.com/fwlink/?linkid=43970) is updated regularly; it is a good idea to check it often for new management packs. Microsoft provides a utility that compares the versions of your installed Microsoft management packs with what is available at the Management Catalog. This utility, the Microsoft Management Pack Notifier, is discussed in the "Management Pack Notifier Management Pack" section later in this chapter. The MP Notifier automates the task of checking for new versions of installed management packs.

The Management Pack Catalog lists management packs for MOM 2005 and other versions of Operations Manager. MOM 2000 management packs are 100% compatible with MOM

2005, although they do not take advantage of new functionality such as reports, state views, and a number of other features.

Management Pack Versions

Implement the MOM 2005 version of a management pack whenever one is available. Many MOM-related issues called into Microsoft Services and Support (formerly known as Product Support and Services or PSS) are from using an outdated version or selecting a management pack written for MOM 2000 rather than one designed for MOM 2005.

Determining Management Pack Versions on Microsoft.com

For any particular management pack, the management pack catalog listing includes a description of the management pack and a link to its vendor's website. The management pack description may include its version. Figure 13.2 shows the management catalog listing for the MOM 2005 management pack.

Product	Description	Company	Last Updated
Operations Manager (MOM) 2005	Allows you to proactively manage your MOM 2000 SP1 and MOM 2005 environments, increasing availability, security, and (MP version: 05.0.2803.0000).	Microsoft	08/31/2005

FIGURE 13.2 Management pack listing.

Clicking on the link to the management pack (in this case the MOM 2005 MP) takes you to the download center page for that management pack. Information at the download center includes the name and size of the downloaded file and its published date and version, an example of which is shown in Figure 13.3.

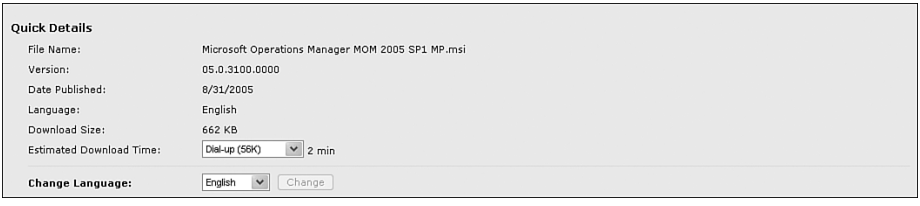


FIGURE 13.3 Quick Details for a management pack at the Download Center.

Quick Details Information

Quick Details information is available for management packs developed by Microsoft; management packs from third-party vendors may not follow this convention.

The functionality described in the management packs covered in this book is based on the versions of those management packs available during mid-2006. Management packs are periodically revised, often more frequently than the corresponding product. It is best to keep up-to-date with the latest release of a management pack so that you will have the latest bug fixes and any improved monitoring routines.

Checking the Version of an Installed Management Pack

To determine the installed version of any management pack, select the top-level rule group of the management pack in the Navigation pane of the Administrator console and right-click, displaying its property sheet. The version number is in the middle of the General tab, as shown in the example in Figure 13.4.

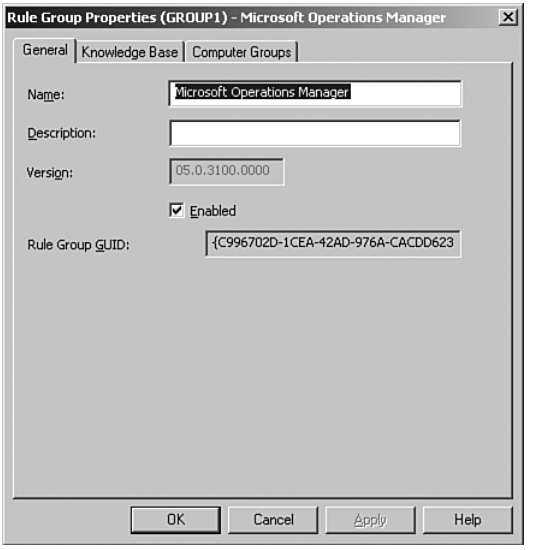


FIGURE 13.4 Checking the version of an installed management pack.

Management Pack Version Numbers

Management packs written for MOM 2000 do not include version information and typically show a version of 00.0.0000.0000.

Planning for Deployment

Deploying management packs involves planning, evaluating in a preproduction or limited production environment, and importing and exporting management packs. Just as you evaluate a new software program before deploying it into production, you should assess management packs before importing and deploying them across your production environment.

Testing gives you an idea of how the management pack operates, what monitoring features are important in your environment, and any additional configuration that may be needed for the management pack. Testing may also reveal possible adjustments you will want to make to performance thresholds. After testing, tuning, and configuring a management pack, you will export it from your preproduction environment and import it into your production system.

Only Install the Management Packs You Need

We suggest installing only those management packs you need. Extra rules can increase the memory utilization of the agents targeted by the management pack and traffic between the managed computers and the management server.

Determine an Order to Implement Management Packs

When planning management pack deployments, a first consideration would be deciding which ones you want to deploy, and in what order. Some applications have dependencies on others, so you may want to implement the related management packs as you deploy those products. For example, say that you use Exchange Server. Exchange requires Active Directory, which in turn utilizes DNS. Another consideration is where you might get the most "bang for the buck"—which management packs will give you the most benefit in the least amount of time. Typically this would be examined from a functional viewpoint. Let's look at two examples:

- You may decide that monitoring Active Directory is a high priority in your environment. Monitoring directory services would best be accomplished by using the Active Directory (AD), DNS, and Group Policy management packs. You might also consider implementing the Windows Server management pack as part of this, or perhaps prior to any of the other management packs.
- Alternatively, you may decide to focus first on monitoring your messaging environment. This would include using one or more of the Exchange-related management packs. As we mentioned, Exchange has dependencies on Active Directory, so monitoring Exchange could include monitoring AD.

The order in which you implement management packs really depends on the priorities of your organization and your goals for monitoring.

Implementing Management Packs

It is best to deploy a single management pack at a time. This practice makes it easier to deal with management pack issues as they occur. When you have more than one management pack involved it may be difficult to determine what initially caused a problem.

Initial Tuning: Tuning By Function

Let's presume that you have determined your strategy and order for deploying management packs and have started importing selected management packs one at a time into your preproduction environment. As part of your approach you should refer to that MP's management pack guide. Each management pack guide discusses particulars for installing, configuring, and tuning that particular management pack. The management pack guides are available at http://go.microsoft.com/fwlink/?linkid=49776, and are often included in the download package with the management pack.

Importing Management Packs

The process of importing management packs is described in the "Importing Management Packs" section later in this chapter.

You will want to do some initial tuning because testing and tuning in a nonproduction environment is always advisable prior to unleashing something new into production. Testing at this point also helps minimize the information load and unnecessary work for your production computer operators.

After evaluating a management pack's behavior you may decide to tune one or more rules to meet your organization's needs. For example, you may find a performance rule generating an alert at a threshold value inappropriate for your environment.

Managing Alerts

As you implement a management pack, it will generate alerts that you will want to review and evaluate for tuning. Some rules may generate low severity alerts; depending on your environment these may not be worth investigating or resolving. In these cases you may consider disabling the rule. Remember that you can document your actions using the Company Knowledge section of the rule.

A suggested approach to tuning a management pack is to work on a server-by-server basis, tuning from the highest severity alerts and dependencies to the lowest. For example, if your plan is to monitor DNS, Active Directory, and Exchange you would first implement the DNS management pack because Active Directory and Exchange are dependent on DNS.

Open the Operator console and change the group scope at the top to either Microsoft Windows 2000 DNS Servers or Microsoft Windows 2003 DNS Servers, depending on which version of DNS is installed. (If both exist start with one and then move onto the other.) Select the State view (shown in Figure 13.5) to identify issues needing attention.

Although the Alerts and Events views typically are the easiest way to see what is going on, the State view is a better method for monitoring and seeing the high-level health of the organization. Using the State view here exposes the servers running DNS and any associated alerts. Double-click on each system you want to examine; then start at the top of the list for each computer and evaluate the alerts in order of their severity (Service Unavailable, Critical, Error, or Warning).

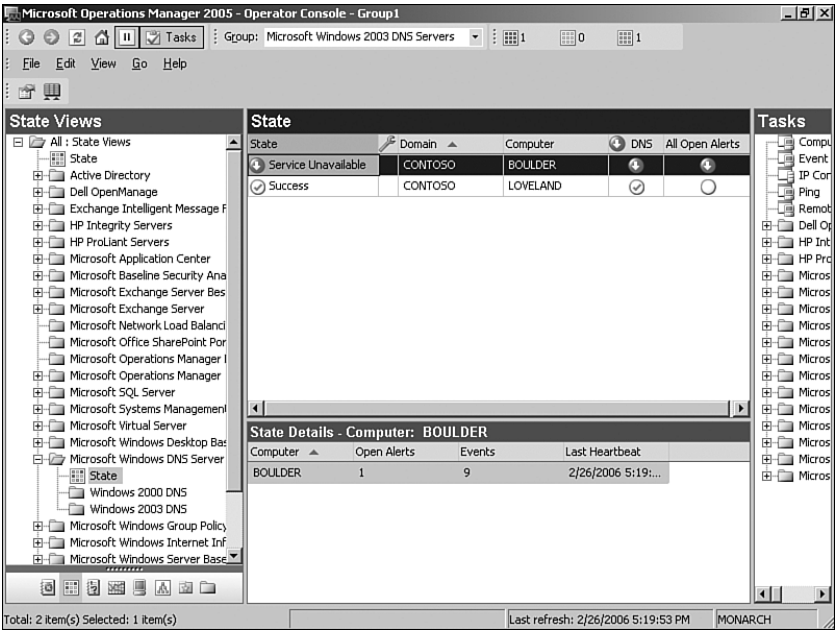


FIGURE 13.5 Checking the DNS Server state.

You should also investigate what events are sent to the management server. Review the Operator console regularly to see whether events are captured that are unnecessary for your environment because this could take up an excessive amount of storage within MOM. Use the Administrator console to disable unnecessary events, change event thresholds, or collect information on a consolidated basis. Microsoft also provides several scripts in the MOM 2005 resource kit that you can use to identify your most common alerts and events. These are the `MostCommonAlerts.sql` and `MostCommonEvents.sql` scripts.

Where Does That Data Go?

Remember that everything seen here takes up space somewhere in the MOM database, so if the information is not relevant you should adjust the underlying rules or conditions so that it is no longer collected.

After you have resolved alerts and events in each function and management pack, implement the next management pack on your list. In our example that would be Active Directory, and then finally on to Exchange. Import the management pack, and after it is functional, work through the Operator console, changing the viewing scope as discussed previously for the DNS servers.

Monitoring Database Space

Another aspect of monitoring MOM is tracking space utilization of the OnePoint and SystemCenterReporting databases. As discussed in Chapter 10, “Complex and High

Performance Configurations," you can use the SQL Enterprise Manager to determine how much free space exists in each database on a regular basis.

If you are using the SQL Server Management Pack (discussed in Chapter 18, "Database Management"), you can have MOM alert you when free space drops below a defined threshold. You will want to monitor space utilization in both your test and production environments.

You may also want to investigate the MOM Database Tracking MP which we include as content with Chapter 18.

After you reach a comfort level with each management pack, it is time to put it into production. Because you have already "tuned" the MP and want to keep your changes, export it from the test environment and then import your version of the management pack into production. We discuss the processes of exporting and importing management packs in the "Exporting Management Packs" and "Importing Management Packs" sections later in this chapter.

Tuning Tips

Although the next few chapters of this book will provide specific tips for testing particular management packs, here are some general guidelines:

- Review any new alerts reported for the servers monitored with the new management pack. MOM Reporting includes several reports to help you discover your most common alerts (including by Severity by Computer Group, Most Common by Alert Count, Most Common by Computer, and Most Common by Computer Group). These reports are in the Operational Health Analysis folder under Microsoft Operations Manager Reporting. If alerts are occurring there are several actions to consider:
  - *Resolve the issue generating the alert.* View the product knowledge base information regarding the specific error occurring in your environment. Typically when a management pack is first installed, it discovers a multitude of previously unknown issues in your environment. Monitor the alerts to determine potential areas of concern.
  - *Override the rule.* MOM 2005 allows you to override the configuration of a rule for a particular computer or all members of a specific computer group. For example, you may want to set individual free space thresholds for specific databases when they are of significantly different sizes.
  - *Disable the rule.* Go to the specific rule for that management pack in the Administrator console; open the properties sheet for that rule, and under the General tab, uncheck the box This Rule Is Enabled. You should only disable a rule after concluding that the issue is not severe enough to warrant an alert and you do not need to be made aware of the specific situation monitored by the rule on any server in your management group. Some rules are initially disabled when delivered in management packs because they may not apply in all situations. (An example of this is the SMS Management Pack where the SQL

Server monitoring rules are initially disabled because the SQL Server MP checks for similar events.)

- *Change the threshold* of a rule that is generating the alert when you want the underlying condition to be monitored, but the rule is generating an alert before the condition is actually an issue for your particular environment. Consider this option if the rule is not a good candidate for an override or disable/enable. An example of where this may occur would be free space thresholds for databases monitored by the SQL Server management pack.

Which Rule Is It?

You can identify the rule by opening the alert in the Operator console and looking in the Details pane in the bottom right-hand section of the Alert Properties page. The Details pane gives you the location to navigate to in the Management Packs section of the Administrator console.

- If a new management pack generates many alerts, you may want to disable rule groups or perhaps individual rules within a management pack. You can turn them on gradually, making the new management pack easier to tune and troubleshoot.

Troubleshooting Management Packs

If a management pack does not appear to function properly, refer to the management pack guide or included documentation for configuration requirements. For example, you will want to verify that the MOM Agent Action account has the appropriate privileges needed for that management pack.

If logging is enabled, you may be able to determine what the issue is based on specific log entries. For more information on logging and locations of the log files, see Appendix A, "MOM Internals."

Remember after making any changes to management packs or rules to Commit Configuration Changes to apply those changes immediately.

How Long to Tune?

There is no simple rule on how long to tune a management pack. Evaluate and tune each management pack until you are comfortable with its functionality and behavior. This may include resolving any outstanding alerts that are not actual problem indicators or adjusting underlying rules and alerts for issues that aren't significant in your environment. You probably will want to go through a full application production cycle for your applications in each area being examined:

- For example, if you are tuning the SQL Server management pack and you have heavy month-end processing activity, go through a month-end cycle to see whether MOM turns up anything unexpected.

- Gauge the effect of any new application added to your environment. Are new alerts being generated?
- Tune and test the impact of any new management pack or new version of an existing management pack.

After completing initial tuning, you may want to further tune management packs after they are in production or when new applications are introduced into your server environment.

Troubleshooting Review

To recap some of the key approaches to managing management packs:

- Introduce management packs one-by-one into your management group, to more easily isolate changes in performance and behavior.
- Only install management packs you need. Management packs increase the load on the management server(s); they also increase the size of the agent on any computers targeted by the management pack.
- Work with your in-house experts for each application to understand how the rules will function in your particular organization; you may decide to disable some rules or change thresholds that would trigger an alert. Thresholds are in the state properties of an alert. (The structure of an alert is described in Chapter 14.)
- Identify rules that are generating the most activity and focus on understanding what is taking place. If MOM Reporting is installed and you are collecting data, Microsoft provides reports you can use to start investigating your most common events and issues, found under Microsoft Operations Manager Reporting \ Operational Health Analysis. Figure 13.6 lists the Operational Health Analysis reports available with MOM 2005.

Determine How Much Data You Are Collecting

A quick way to find out how many event and performance records are in OnePoint is by running these two SQL queries:

```
select count(*) as count from sdkeventview
select count(*) as count from sdkperformanceview
```

- Look for Queue Full alerts that MOM may generate, an example of which is shown in Figure 13.7. Queue Full alerts may be associated with Event IDs of 21268, 22061, 22062, or 21269. The alert typically occurs if processing is blocked for more than 60 seconds. The queue may be full on the agent or on the management server, and the error may be caused by either the agent not being able to communicate with the management server or a Data Access Service (DAS) issue on the server preventing insertion of data into the database. It may also indicate that the volume of data

being queued to transfer to the management server has exceeded the capacity of the temporary storage area (queue). The error tells you which server(s) are generating the most events. If there seems to be a high volume of activity, check the event log of those servers to find out whether something is occurring that would cause the queue to fill up.

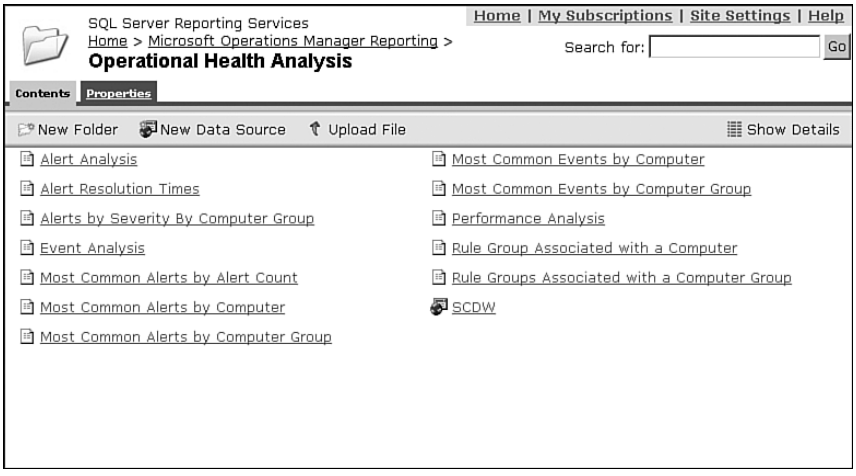


FIGURE 13.6 Operational Health Analysis reports.

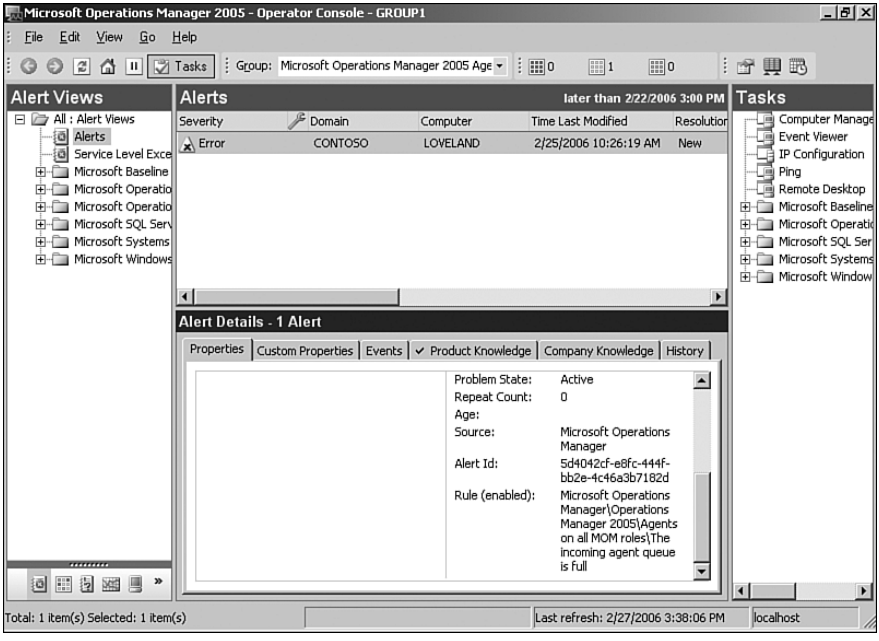


FIGURE 13.7 The incoming agent queue is full.

If you receive the Queue Full error on the management server with an Event id 22061, check http://support.microsoft.com/kb/901049/. This article includes an in-depth discussion regarding this particular occurrence.

After resolving the cause, you may run into a deadlock situation when clearing out the queues. As MOM is trying to clear out the queues, scripts are trying to write additional data but cannot because the queue is already full. Hotfix 900333 is available for this situation, which is described at http://support.microsoft.com/kb/902447/.

Real World—The Queue Is Full Error

A stopgap approach to dealing with a full queue is to increase the temporary storage settings on the affected server. This is not recommended other than for debugging purposes. Increasing the queue size is only a short-term solution; if the underlying problem is not corrected the queue eventually fills again.

One situation where it makes sense to change the temporary storage settings is when you have a planned network outage. In the Administrator console go to Administration \ Computers \ All Computers, and in the Detail pane select the server indicated in the error. Right-click to bring up the Properties sheet and select the Temporary Storage tab. If the computer is configured to Use Global Settings uncheck that option and then adjust the Temporary storage settings. Figure 13.8 shows the Temporary Storage screen for a management server.

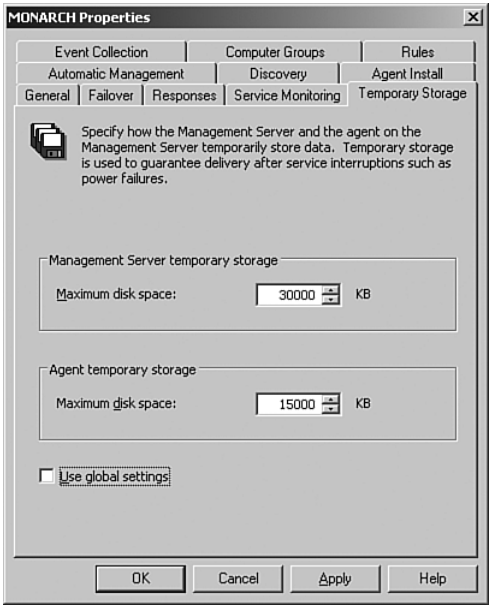


FIGURE 13.8 Change the temporary storage setting.

Restart the MOM service on any servers for which you change storage settings.

After you identify the system generating the messages, you need to determine which rules are using those events and how to resolve unnecessary events—which can include disabling rules, using overrides, changing thresholds, or utilizing consolidation rules.

Now that we have discussed some initial approaches for tuning your management packs, let's look at the process to move management packs with their changes from a preproduction environment to a production environment. Remember, the recommended approach for implementing management packs is to test them in a preproduction environment, make tuning changes as necessary, and then import the modified management packs to your production MOM 2005 environment.

Exporting Management Packs

The Import/Export Management Packs Wizard in the Administrator console is the mechanism typically used in moving management packs between management servers. Use the Export function to back up or to move management packs from one system to another (such as from your test environment to production). The export procedure was previously described in Chapter 12, "Backup and Recovery." The Import/Export Wizard can be used to move management between management servers, import new management packs into MOM 2005, or be used in backup and restore situations.

1. Open the wizard in the Administrator console by right-clicking on Management Packs in the Navigation pane and selecting Import/Export Management Packs.
2. Click Next on the Welcome to the Management Pack Import/Export Wizard screen; then click on the radio button to Export Management Packs and continue.
3. On the Select a Rule Group page, you will be asked to select a particular rule group in the rule group to export, as shown in Figure 13.9.

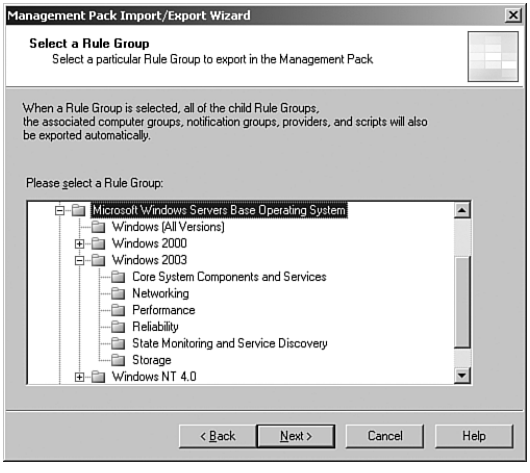


FIGURE 13.9 Select a rule group to export.

Management packs have a hierarchical structure; you can export at any folder level in the structure. All child rule groups, associated computer groups, notification groups, providers, and scripts will also be exported.

4. You are next asked to select the views you want to export as part of the management pack. These views are utilized by the Operator console.

   Navigate to the folder that contains the views that you want to export and select the check box beside those views. You can select a group of views or individual views. If you select a parent node for a view, all the child views for the node are automatically selected, as shown in Figure 13.10.

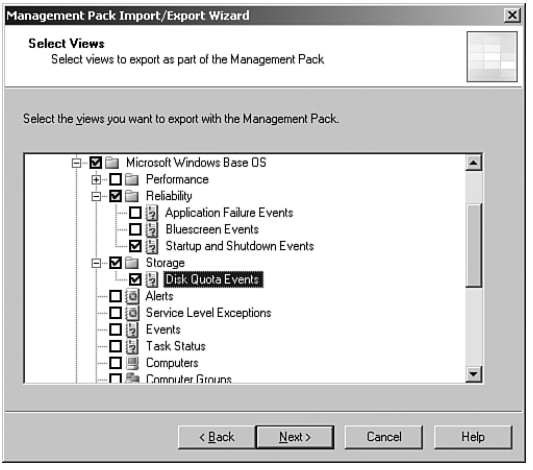


FIGURE 13.10 Select views to export with the management pack.

5. On the Select Tasks page shown in Figure 13.11, specify any tasks you want to export with the management pack.

6. The next page of the wizard asks you to specify the management pack name and location where you will export the management pack. You can type in the export location or browse to it. Management packs are exported into a file with an .akm extension.

   If a file already exists with this name, you are asked to specify how to handle overwrites. Options include the default of overwriting the existing management pack file or appending to the existing file.

   If you developed the management pack using authoring mode, you can also specify whether the type is full or retail.

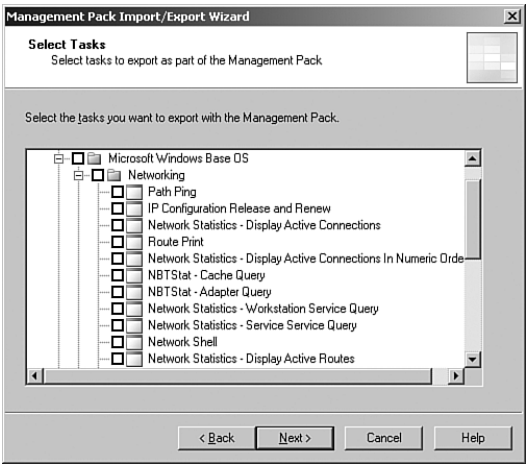


FIGURE 13.11 Select tasks to export with the management pack.

Exporting Management Packs Developed Using Authoring Mode

Management packs developed in authoring mode can be exported specifying a mode of full or retail. When you export the full management pack, the knowledge base can be edited, and rules marked for deletion are included with the export. Full is the default option. A Retail export drops any rules marked for deletion, and the knowledge base is read-only.

More information on developing management packs is available in Chapter 20, and in the *Microsoft Operations Manager (MOM) 2005 Management Pack Development Guide*. The development guide can be selected for download at the Microsoft download site, http://www.microsoft.com/downloads, by searching for "MOM 2005 development guide."

7. At the Completing the Management Pack Import/Export Wizard screen, review your options and click Finish to export your management pack. The Export Status screen shows the status of each component you selected for export. Click Close when the export is complete.

After exporting the management pack from your test environment, your next step is importing it to a production management server and integrating the management pack into the targeted management group.

Importing Management Packs

When importing a management pack, you can update an existing management pack or replace it with the new version:

- Replacing a management pack completely removes the previous version of that management pack from your management server, overwriting it with the new version. Replacing a management pack is suggested only when you do not need to retain any previously created company knowledge or custom rules.
- The Update option retains any information added to the company knowledge base, if you enabled or disabled any rules, and any custom rules added to the management pack. Any other changes (including modified rules, scripts, data providers, or computer groups) are overwritten.

The Administrator console is used to replace or update a management pack. There is also a command-line utility, ManagementModuleUtil.exe, described in Chapter 12. The command-line tool gives you the ability to automate the import and export functions.

When using the Administrator console to import a management pack to replace a previous version, select the option to back up the existing management pack. A backup gives you the ability to easily revert back to the prior version should that become necessary. Management pack backups are located in the *%ProgramFiles%*\Microsoft Operations Manager 2005\MPBackupDir folder and have an extension of .akm.

Tips for Importing Management Packs

Remember Murphy's Law that if anything could go wrong, it might where humans are involved! To minimize the impact of human error, keep these tips in mind:

- Only replace an existing production management pack with one you have checked out in your test or preproduction environment.
- In the Import Wizard, always select the option to Back Up Existing Management Pack, enabling you to return to your former management pack state by importing the backup should that become necessary.
- If you modify any of the original vendor rules, it is best to make your changes to a copy of the rule in a custom management pack. By keeping your changes separate, your modifications are not overwritten when you use the update option to import a new version of the management pack. Disable the original rule.

After downloading a management pack through Microsoft's Management Pack Catalog, you will extract the contents of the package into files that can be utilized by MOM. Copy the executable package to a system with the MOM 2005 Administrator Console installed and run the package to extract the files to the file system.

Packages contain one or more management packs (with an extension of AKM) and reports (XML files), if they exist for the management pack, and may include documentation such as a management pack guide or readme file.

Extracting Management Packs

Extract to the same server and directory all management packs that you want to import to simplify the installation process later.

Using the Administrator Console

To import a management pack, open the Administrator console and select Management Packs in the Navigation pane; then choose the Import Management Packs option in the Detail pane. This starts the Management Pack Import/Export Wizard.

1. Click Next on the Welcome to the Management Pack Import/Export Wizard screen, and click on the radio button to Import Management Packs and/or Reports to continue.
2. Browse to the directory structure for the management pack(s) and click on the radio button to Import Management Packs and Reports. (You could also use this dialog to Import Management Packs only or Import Reports only.) Click Next to continue.

Importing Reports

Some management packs do not include reports; for these you would select the check box to Import Management Packs only. If MOM Reporting is not installed, the import tool will not display reports as part of the selection to be imported, even if they are part of the downloaded package.

If you plan to use MOM Reporting, we recommend you install it prior to importing management packs, so you can import both at once.

3. At the Select Management Packs step, highlight the management packs(s) you want to import.

   Options include updating the existing management pack or choosing to entirely replace your existing management pack. You can also elect to make a backup of the current management pack. The wizard defaults to the selections of Update Existing Management Pack and Back Up Existing Management Pack. Choose the appropriate option(s) for your environment and click Next.

Differences Between Updating and Replacing a Management Pack

The Update option preserves the current enabled/disabled rule configuration, any new rules and groups, and any company knowledge base entries. If you choose the Replace option, all customizations are lost. We cannot repeat too strongly to always select the Backup option when a prior version of the management pack is installed, unless you want to undo any changes you have made.

4. If you selected the Import Reports or Import Management Packs and Reports option earlier, highlight the reporting file(s) to import and then click Next to continue.
5. If a Secure Socket Layer Confirmation screen appears, click Continue.
6. Click Finish on the Completing the Management Pack Import/Export Wizard screen to complete the process.

The Import Status screen appears and provides status of the management pack installation. Click Close at the bottom of the screen when the installation is complete.

Using the ManagementModuleUtil Tool

The ManagementModuleUtil utility is a command-line tool installed with MOM 2005 that can import or export management packs. The utility does not automatically back up an existing management pack; to perform a backup yourself, manually export the management pack as your first step. ManagementModuleUtil was previously discussed in Chapter 12.

Deploying Changes

Changes to a management pack automatically propagate after attribute discovery, group membership, or an agent request for a configuration change occurs. To immediately deploy the management pack, commit the changes to your MOM configuration, thereby propagating the configuration changes to all management servers in your management group. To commit changes, right-click on the Management Packs node in the Navigation pane of the Administrator console, and select Commit Configuration Change. You will get a confirmation message as shown in Figure 13.12.

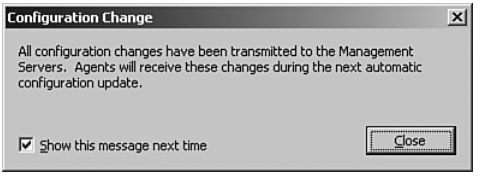


FIGURE 13.12 Commit a configuration change.

After configuration changes are transmitted to your management servers, the changes are sent to the agents themselves during the next automatic configuration update. By default, the Agent Request configuration interval is 1 minute, which is the lowest possible setting for agents to receive updates. The configuration interval is located in the Administrator console under Global Settings \ Agents \ Agent Heartbeat tab \ Configuration Requests.

Information on Agents

MOM Agents are discussed in Chapter 9, "Installing and Configuring Agents."

Verifying the Management Pack Installation

After installing a management pack, you will see changes in the various MOM consoles:

- In the Administrator console under Management Packs, the Computer Groups folder now includes groups related to the particular management pack. Under Rule Groups, a folder structure is created for the management pack. There may also be new Scripts, Notification Groups, and Data Providers.

- In the Operator console there may be additional View Folders and Views for exposing Alerts, Events, or Topologies.
- In the Operator console in the State view, there may be new column(s) associated with the new management pack.
- If MOM Reporting is available in your system and the management pack import included reports, the Reporting console lists reports for the new management pack and possibly subfolders as well.

Real World—Deleting Management Packs

Removal of management packs is a more complicated process than adding them. There is no completely clean process to remove a management pack (this is on the wish list for the next release of Operations Manager), but the following removes most of a management pack:

1. Mark all of the rule groups as disabled and wait one week. The "one week" time period is because a rule group can't be deleted until MOM has groomed out any live data related to that management pack. If you have a four-day retention period before grooming, you would wait four days.
2. Delete the rule group(s).
3. Delete the computer group(s).
4. You can delete any scripts that were used as part of the management pack—but be careful! Verify that the scripts are not used by any other rules.

Knowledge base article 918278 also discusses several methods to uninstall management packs; see http://support.microsoft.com/kb/918278/.

Perhaps the easiest way to keep a management pack from functioning is through disabling the computer groups it uses (if they are not used elsewhere) or disabling its rule groups. Making a management pack nonfunctional is less work and a less risky process than actually deleting it.

Finding KB 918278

You may receive a message that The Knowledge Base (KB) Article You Requested is Currently Not Available when you look for article 918278, referenced in the preceding sidebar. This is because Microsoft has at least temporarily pulled the article. But never fear, you can also reference it at http://blogs.msdn.com/incarnato/archive/2006/05/18/601309.aspx. This particular blog is maintained by Justin Incarnato of the MOM Team.

Managing Management Packs

Now that we have covered some information about how management packs work and the import/export process, we will look at several utilities for managing management packs.

With the exception of the Management Pack Notifier, these utilities are part of the MOM 2005 Resource Kit.

On the CD

You can find the MOM 2005 Resource Kit on the CD included with this book.

Management Pack Notifier Management Pack

One of the challenges in managing MOM is knowing when there are updates to management packs you are using. The Management Pack Notifier Management Pack determines the versions of your current management packs and compares them with the versions currently available at the MOM management pack website. The Management Pack Notifier uses Information Alerts to notify you if there are updated versions of the management packs that you have installed.

Using the MP Notifier

The Management Pack Notifier does not work with management packs designed for MOM 2000 because they do not include version numbers.

The Management Pack Notifier MP includes the following functionality:

- Determining which management packs are currently installed.
- Checking the Microsoft website to determine whether updated versions are available. The MP Notifier compares the version numbers from Microsoft with the installed version numbers.
- Generating an Informational Alert if an updated version is available from the Microsoft website.

Locate, Download, Install

The Management Pack Notifier can be found on the Microsoft Management Pack catalog at http://go.microsoft.com/fwlink/?linkid=43970.

Download the .msi file of the Notifier and install it on your MOM 2005 server. The .msi has three files including an .AKM file (the management pack), a Readme file, and an End User License Agreement (EULA). There is no management pack guide for the Management Pack Notifier. Import the .akm file into your MOM environment using the process described earlier in the "Importing Management Packs" section of this chapter.

Configure

Importing the management pack creates a rule group and a computer group. For the management pack to function, you must add a management server to the Microsoft

Operation Manager MPNotifier MOM Server computer group. The specified server must have Internet access to be able to send an http request to the Microsoft website.

Configuring for a Firewall

If your organization has a firewall, make sure that the web browser settings on the server you will be using include appropriate proxy information.

To receive notifications of which management packs have posted updates you must add users to the Operations Manager Notification group. This group is found in the Administrator console under Management Packs \ Notification Groups \ Operations Manager Notification Testing.

Rules and Alerts

The rules in this management pack provide the following functionality:

- Check MOM Versions (runs every 24 hours)—The Microsoft MPNotifierVersion Check script determines what versions of management packs are installed.
- Alert when Versions don't match—Checks for event id 1002 from the MOMMPVersionCheckMP section of the event log.
- Alert MOM Admins of any new versions—Alerts the Operations Manager Administrators in the Operations Manager Notification notification group when new versions of management packs are available.

Differencing Tools

The Management Pack Differencing Tools are part of the resource kit. You can use either a graphical user or a command-line interface. Both tools generate an XML report of what was added, deleted, or changed between two versions of a management pack (referred to as source and destination). The management pack must be in XML format; you can use the resource kit MP2XML.exe tool to convert management packs to XML.

The syntax for the command-line version (MPDiff.Console.exe) is

```
MPDiff.Console.exe <required> [<optional>]
<required>
/src:            The source ManagementPack XML file.
/tgt:            The target ManagementPack XML file.
[<optional>]
/lock:           Apply a lockfile against the diff result.
/createLock:      Create a lockfile from this diff result.
/schema:         Whether to validate against MOM XSD (default is 'on')
/out:            The XML diff result file to output (default 'diffout.xml').
/v:ucad          Verbosity level, where u=unchanged, c=changed, a=added, and
d=deleted items. Items can be chained. Example: "/v:cad".
```

The command-line interface enables you to automatically generate a report that uses Extensible Stylesheet Language Transformations (XSLT) to create an HTML table. You can also create lock files to keep track of changes in the management pack. First you would use the `/createLock` argument; you can later run the utility with the `/lock` argument and be informed of any changes in the new XML version of the management pack.

Using the graphical user interface (MPDiff.exe) allows interactive viewing of the differences between the source and destination management packs.

Rule and Group Toggle Utility

The Rule and Group Toggle utility is a handy command-line tool you can use for enabling or disabling computer groups, rule groups, or rules—specifying these either by name or by GUID. The syntax for RuleUtil.exe is

```
RuleUtil.exe <Action> [<Specifier>] [<Option(s)>]
<Action>
/list:[<all/computer/rule>] Lists computer or rule groups, default all.
/enable     Enables the specified computer or processing rule group.
/disable    Disables the specified computer or processing rule group.
/commit:[<true/false>]  Commits any changes, default true.
<Specifier>
/compgroupname:<name>    Specifies the name of the computer group.
/compgroupid:<id>      Specifies the id of the computer group.
/rulegroupname:<name>    Specifies the name of the computer group.
/rulegroupid:<id>      Specifies the id of the computer group.
<Option(s)>
/r          Lists subgroups as well as top level groups, only valid with the 'list'
action.
```

You can use RuleUtil in a batch mode to enable or disable rules and groups.

Resultant Set of Rules

Resultant Set of Rules (RSOR.exe) is a command-line utility that lets you—surprise, surprise—view the resultant set of rules that are targeted to an agent. The utility communicates directly with the MOM database using an ActiveX Data Object. The syntax for RSOR is

```
RSOR.exe <MOMDBServer[\instance]> <TargetAgent>
<MOMDBServer>    name of the database server hosting the OnePoint database
[\instance]      specify the instance name if not the default instance
<TargetAgent>    name of the managed computer whose rules you want to obtain
```

The output from RSOR is a text file created in C:\ResultantSetOfRules, with a naming convention of *COMPUTERNAME* RSOR *YYYY-MM-DD HHMMSS*.log.

Computer Group Hierarchy Import and Export

Another resource kit utility is the Computer Group Hierarchy tool (CGHUtil.exe), which allows you to export a Computer Group Hierarchy from MOM (or Active Directory) to an XML file and re-create that hierarchy on a target MOM system. The syntax for CGHUtil is

```
CGHUtil.exe <option> <filename> [<extendedOptions>]
<option>
/dump          dump MOM Computer Group hierarchy under specified computer group
/dumpad        dump Active Directory OU Hierarchy starting with specified OU
/create        recreate Group Hierarchy
<extendedOptions>
/WithComputers  includes computers listed in "Included Computers" tab (or computer
objects in respective container in OU hierarchy)
```


Sample CGHUtil commands are shown in Table 13.1.

TABLE 13.1 CGHUtil.exe Examples

Syntax	Result
`CGHUtil.exe /dump CG.xml`	Exports all MOM computer groups to the CG.xml file.
`CGHUtil.exe /dump CG.xml "Microsoft Operations Manager 2005 Agents"`	Exports any hierarchy under the Microsoft Operations Manager 2005 Agents computer group.
`CGHUtil.exe /dump CG.xml "Microsoft Operations Manager 2005 Agents" /WithComputers`	Exports any hierarchy under the Microsoft Operations Manager 2005 Agents computer group in addition to computers listed in the Included Computers tab for this computer group. When the re-create step is run, the Included Computers tab is also restored with this file.
`CGHUtil.exe /dumpad CG.xml LDAP://OU="Managed,DC=contoso,DC=com"`	Exports the OU hierarchy starting from an OU named “Managed” in the contoso.com domain.
`CGHUtil.exe /dumpad CG.xml "LDAP://OU=Managed,DC=contoso,DC=com" /WithComputers`	Exports the OU hierarchy starting from the “Managed” OU in contoso.com, and also exports computer objects in each respective container. When the re-create step is run, these computers will be added to the Included Computers tab for each computer group created.
`CGHUtil.exe /create CG.xml`	Re-creates the computer group hierarchy exported to the CG.xml file. It does not create new computer groups. It looks for existing computer groups that match,and re-creates the relationships required to establish the right hierarchy that was exported.

TABLE 13.1 Continued

Syntax	Result
`CGHUtil.exe /create CG.xml /WithComputers`	Re-creates the computer group hierarchy exported to the CG.xml file. It uses computer information, if existing in the export file, to make it part of the Included Computers list for that computer group.

If you omit the optional Computer Group Name or use "All," a hierarchy of all groups is used. If you omit the optional Computer `/WithComputers` switch, no information about computers is dumped or used.

Using the MOM 2005 Resource Kit

Remember that the MOM 2005 Resource Kit is not officially supported by Microsoft.

Summary

In this chapter you were introduced to management packs and tuning techniques. We discussed the process to implement management packs and best practices for deployment. In the next chapter we will look at how MOM monitors managed servers by using the various rule types you find in its management packs. We also discuss monitoring tips and techniques to use with MOM 2005

CHAPTER 14

Monitoring with MOM

IN THIS CHAPTER

Microsoft Operations Manager (MOM) is designed to provide monitoring for applications, operating systems, and networking devices, using both Microsoft and third-party management packs. This chapter discusses several major components of MOM including rules, alerts, resolution states, and the knowledge base.

Rules define what conditions should be monitored on the server(s) where they are applied. Rules represent the fundamental business logic; they indicate what data to collect and how to respond to that information. *Alerts* call attention to issues requiring administrator attention or issues with server performance. *Resolution states* indicate the current condition of a specific alert. Finally, the *knowledge base* provides product information to assist MOM administrators in resolving issues identified in the MOM environment.

This chapter discusses the types of rules that exist in MOM 2005 and the process of creating rules. We cover how rules and alerts function, how resolution states work, and the role of the knowledge base. We will also discuss tips on using MOM for monitoring purposes and investigate the process of troubleshooting rules and alerts within MOM 2005.

Why Monitoring Is Important

MOM gathers information from a variety of sources (event logs, performance counters, application log files, Simple Network Management Protocol [SNMP] traps, syslog information, Uniform Resource Locator [URL] monitoring, and Windows Management Instrumentation [WMI] events), and is designed to tell you whether issues are found. When a server managed by MOM is operating without problems,

it will not generate messages in the Operator console. If a problem occurs or a threshold is exceeded, MOM 2005 can perform a variety of responses including generating an alert, sending an email, running a script, or undertaking other actions discussed later in this chapter.

MOM also executes responses to situations that require attention. For example, MOM can restart a stopped service, run a script to increase the amount of free space on a drive by deleting files, or notify the owner of an application that an issue needs to be resolved. Monitoring is important because it provides detailed insight into the state of your infrastructure, facilitating proactive actions to resolve issues before they impact users.

MOM deployments with multiple management packs may have thousands of rules, and most of these rules can generate alerts, resulting in potentially thousands of alerts. The quantity of possible alerts makes it vital for alerts to be generated only when actual problems are identified that require resolution. Restricting the number of alerts is important to avoid alert overload, which can occur if you overwhelm your operations staff and administrators with alerts. When people receive too many alerts over time they tend to start ignoring them (also known as the *crying wolf syndrome*).

An Approach to Minimize Alerts

As discussed in Chapter 13, "Administering Management Packs," we recommend that you install and test each management pack individually to tune out any unnecessary alerts.

Reviewing Alerts

When you implement MOM in your production environment, we recommend that you also implement a process to review the alerts generated by MOM. One approach for doing this is through an alert review. During an alert review, the group(s) responsible for the applications receiving the alerts review all generated alerts. The alert review should also identify situations where MOM did not generate an alert but should have done so.

Rules

MOM does nothing unless told to. Without the rules that ship in the management packs, MOM would do nothing until you created a rule. Thankfully, the product ships with a huge investment in rules written by Microsoft. This helps the product hit the ground running and provides a strong return on investment.

Rules—The Backbone of the Business Logic

The true intelligence of MOM lies in its rule sets. MOM ships with more than 5,000 rules. These rules give the system a detailed playbook of what is okay and what is not with Microsoft's platforms and servers. These rules are the actual orders the agents follow. The

management pack rules were developed by the Microsoft product teams, Microsoft Product Support Services (PSS) and Microsoft Consulting Services (MCS), and are how these teams transferred their gray matter and experience on the various Microsoft products into MOM. The rules cover everything from which events constitute problems, what performance counters are the important ones to monitor, and what the threshold values should be to what reports are most useful to administrators and even how to configure a technology according to best practices.

These rules are centrally created and automatically deployed to the correct computers, based on specific criteria or attributes. This allows rules to be

- Easily created
- Easily deployed
- Applied consistently

The ability to create rules centrally reduces overhead and increases the reusability of components such as data sources or scripts. Automatically deploying rules to groups of computers is powerful because applying sets of rules as a group ensures that the rules are consistently applied and servers are managed in a standard manner. The sets of rules are

- Rule groups
- Management packs

Rule groups are the groups of rules deployed as a set. As discussed in Chapter 13, *management packs* are collections of rule groups and several other associated configuration items, such as views, tasks, and reports. You can think of management packs as supersets of rule groups.

Handling Information

When MOM collects data through its rules, it can respond to that data in a variety of ways. Paradoxically, these are also rules. These responses allow MOM to notify the correct personnel, consolidate the information with previous events, or trigger an automatic action to resolve the alert condition. This capability allows MOM to collect a huge amount of information, yet distill it down to a few sets of items that need to be brought to the attention of an administrator.

A typical reduction of events to alerts would be distilling some 14,879 events generated in a three-day span by 15 computers down to about five error alerts requiring the administrator to take action on (that is, trouble tickets) and about 16 advisory warnings to review. This is approximately 0.03% of total events generating trouble tickets that require administrative action. The 16 advisory alerts would not generate trouble tickets in most environments but are rather there to help you tune and optimize your system; and even these are only about 0.11% of the total events. Figure 14.1 shows the huge reduction of information graphically. You can see the thin slice of alerts when compared to the overall mass of

events. The slice is then expanded, graphically showing the ratio of advisory to actionable alerts.

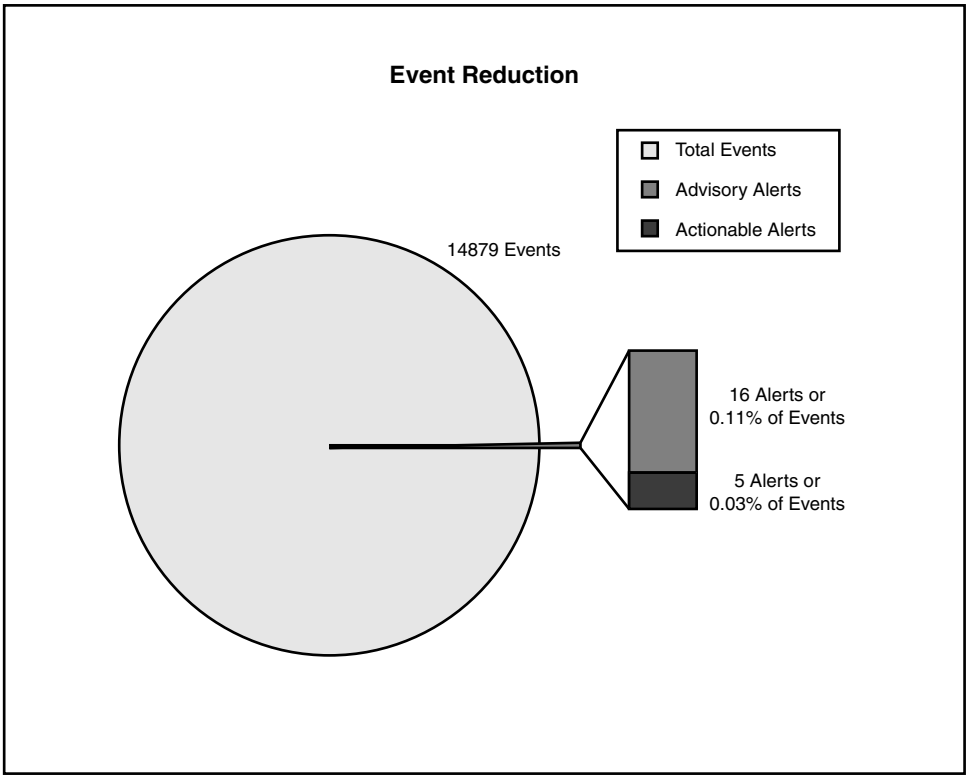


FIGURE 14.1 Event reduction.

This means that the administrator does not have to review the 14,000+ data points generated by all the logs and performance counters on 15 different servers with a half dozen consoles or tools, but can instead focus on the key events likely to need attention using a single console. The majority of the 21 key events (the advisory warnings) are simply proactive warnings of transient utilization peaks and optimization suggestions. For anyone responsible for a group of servers, getting this type of proactive advice is an incredible timesaver!

MOM 2005 has three primary types of rules: event rules, performance rules, and alert rules. We will discuss each type of rule, including the different subtypes for each. We will also discuss how and why each rule type is used.

Event Rules

Event rules act upon events gathered from various providers including the Windows event log, WMI events, MOM 2005 internal or script-generated events, and custom-provider generated events.

For discussion purposes, we will first establish a new rule group as a container for the rules we will create in this chapter. To create a rule group, open the Administrator console and navigate to Management Packs \ Rule Groups. Right-click on Rule Groups and choose Create Rule Group. Enter **RuleTesting** for both the Name and Description fields (as shown in Figure 14.2) and take the defaults through the remainder of the wizard process.

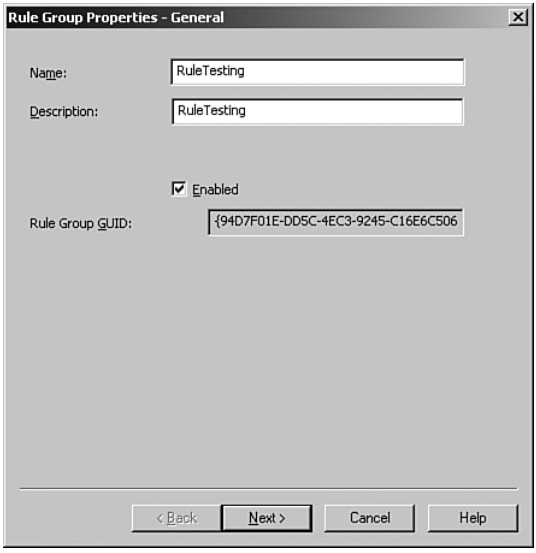


FIGURE 14.2 Creating the RuleTesting rule group.

To create an event rule within a new rule group, open Management Pack \ RuleTesting \ Event Rules. Right-click on the Event Rules folder and choose Create Event Rule in the context menu. Five different types of event rule options are listed, displayed in Figure 14.3.

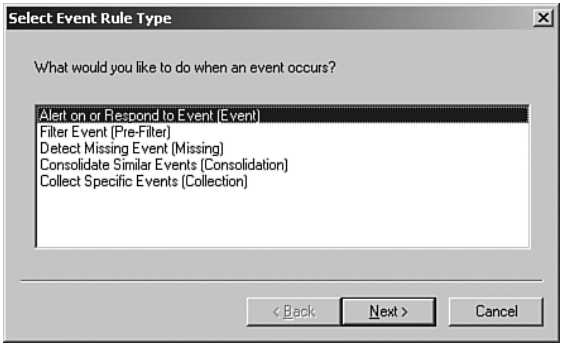


FIGURE 14.3 The five types of event rules.

The different event rule types are

- Collection rules—This type of rule just collects events. Collection rules are useful for reports and troubleshooting. MOM provides event log aggregation, meaning that the local event logs on the servers are centrally collected and stored. Consolidating the event logs makes it easy to generate a report indicating when a user logged in within the past month, based on the security event logs on all monitored domain controllers.
- Missing event rules—This rule type generates an alert or a response when an event has not occurred within a specified time frame. This is useful for detecting events that should have happened but did not, such as backup notifications, scheduled batch jobs, and other automated tasks. Although this is a much-touted event rule type, it is actually seldom used.
- Consolidation rules—This rule type takes a group of similar events and summarizes them into a single event. This is useful if you have a group of events that occur in a short span of time and do not want to clutter the system with a lot of the same type of events. For example, you have an application that runs batch jobs at night and generates 25 print jobs. You need to know that the application completed all its print jobs. Rather than have MOM display all 25 events showing that the print jobs completed, you could consolidate all the jobs into one and test that the count is 25.
- Filtering rules—These rules block events from being stored in the database, in effect filtering them out so that they do not clutter up the database. An example of this might be that you normally collect all application event logs but want to exclude all information events from a really chatty application.
- Event rules—Event rules allow you to generate an alert in response to an event. This is the most common rule type, allowing you to both detect and take action on an event.

The order we have listed these rules is also the order in which the agents process them—that is, collection rules are processed first, missing event rules next, and so on. This is important for understanding what the final effect will be for a given collection of rules. For example, if you have an event rule that you want to generate an alert for each print job and use a consolidation rule to consolidate those jobs, you will only get an alert for the consolidated events. On the other hand, if you create a collection rule to collect print job events, the rules are still inserted into the database individually because the collection rule is processed before the consolidation rule. You would see an event for each print job.

The next sections discuss the event rule types in the order listed in Figure 14.3.

Alert on or Respond to Event

The first rule type listed is the Alert on or Respond to Event rule, which is the most commonly used rule type. This rule type detects a specific event (by source, event ID, type, description, or other criteria) and responds to it. We will select this rule type, starting a wizard that generates the rule. For our example we will create a rule called

Notification of Reboot to provide an alert when a monitored system is brought back online.

1. The first step of the wizard, shown in Figure 14.4, asks you to specify the data provider, which is the source of the event.

   For this example, we will choose the System event log, making the Provider Name System and the Provider Type Windows Event Log. This tells MOM that the event we are looking for is written to the System event log on the managed computer.

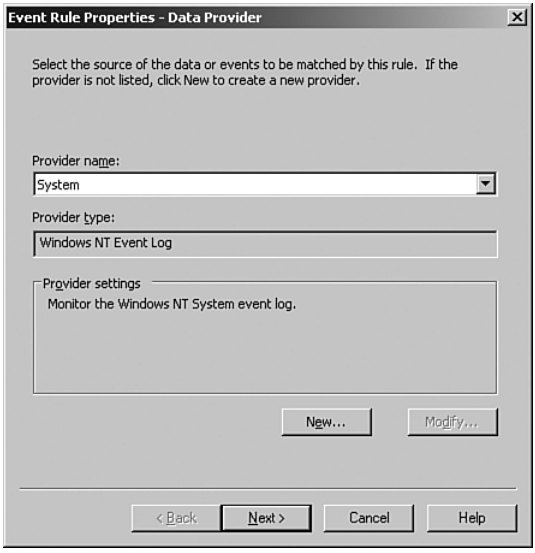


FIGURE 14.4 The Provider screen choosing the System event log within an event rule.

2. Figure 14.5 shows how we can define the event rule criteria. We can specify the event source, event ID number, event type, or event description, or define more advanced criteria. Here we will add a restriction to our selection to include System event log entries with event ID number 6009, which indicates that the event log started and shows the version of Windows running on the system.

Using Criteria to Set Boundaries on the Rule

If the defaults are taken on the criteria page (all options blank), the rule selects every event within the System event log. *This is not recommended because it will store every event from the System event log (on every system that has the rule applied to it) in the MOM database*. It is generally better to set boundaries on the rule to restrict what data is collected.

FIGURE 14.5 Defining the event rule criteria.

Choosing the Advanced button on the event rule criteria brings us to the Advanced Criteria screen, shown in Figure 14.6. This screen offers more in-depth capabilities to determine the criteria to apply to the rule.

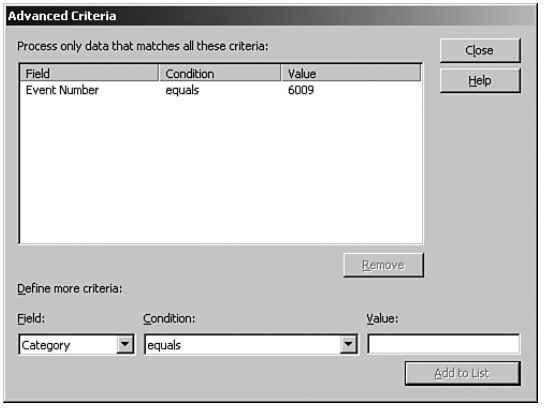


FIGURE 14.6 The Advanced Criteria screen of an event rule.

For example, we can parse the event description and look for a wild card such as a specific computer name to which we want to apply the rule. The criteria we previously specified on the Event Rule Properties page passes to the Advanced Criteria screen so we see the event ID 6009 previously defined.

3. The Schedule Event Rule Properties screen, shown in Figure 14.7, defines when the rule is in effect. The default is to Always Process Data, but there are situations when you may want rules to be in effect only during specific hours. For example, you may create a rule that applies only during business hours Monday through Friday.

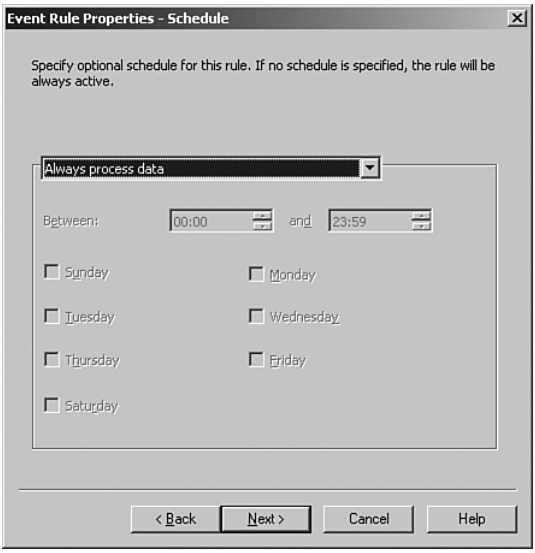


FIGURE 14.7 The Schedule screen of an event rule.

Scheduling Rules

To continue with our example, if we do not want to be notified outside of business hours when a particular system has been restarted, we could configure the rule to only alert on business days during business hours. This scheduling example is shown in Figure 14.8.

4. The wizard proceeds to the Alert Event Rule Properties screen shown in Figure 14.9. On this screen we can configure a rule to generate an alert. Checking the Generate Alert box specifies that MOM generate an alert when Event 6009 is found in the Application event log. This screen allows us to configure alert properties including the severity, owner, initial resolution state, alert source, and description. In this example, we will choose Warning as our alert severity value.

   We discuss more details on this screen and the fields within it in the "Generating Alerts" section later in this chapter.

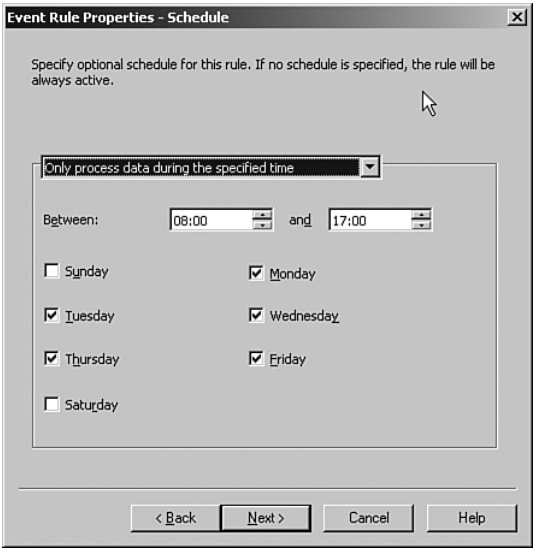


FIGURE 14.8 Schedule a rule to run only during business hours during the week.

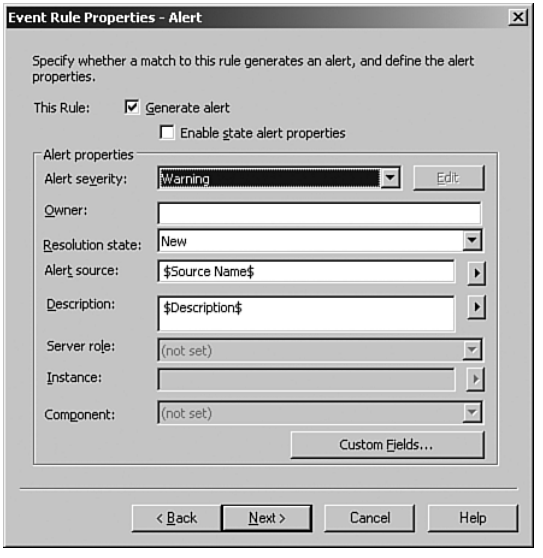


FIGURE 14.9 The Alert screen of an event rule.

5. The next screen is the Alert Suppression Event Rule Properties. This screen gives us the option to suppress duplicate alerts.

Suppressing Duplicate Alerts

Why would you want to suppress duplicate alerts? Let's look at a situation where disk space is running low, generating an alert. If alert suppression is not configured a new alert is generated each time the threshold rule checks counter for Logical Disk\% Free Space. If the Suppress Duplicate Alerts option is checked using the default values, it does not alert each time the threshold rule checks but rather will increment the repeat counter of the alert. The repeat counter shows how many times the alert occurred without filling up the Operator console (or email inboxes of your administrators) with duplicate alerts.

Threshold Rules

We discuss threshold rules in the "Performance Rules" section later in this chapter.

As shown in Figure 14.10, you can choose the fields for suppressing a duplicate alert (options include Alert Name, Alert Description, Alert Source, Severity, Computer, Domain, Source Name, Event Number, Category, Description, Event Type, Message DLL, Message DLL File Version, Provider Name, and User Name). For our example we will use the default options, which are Computer and Domain.

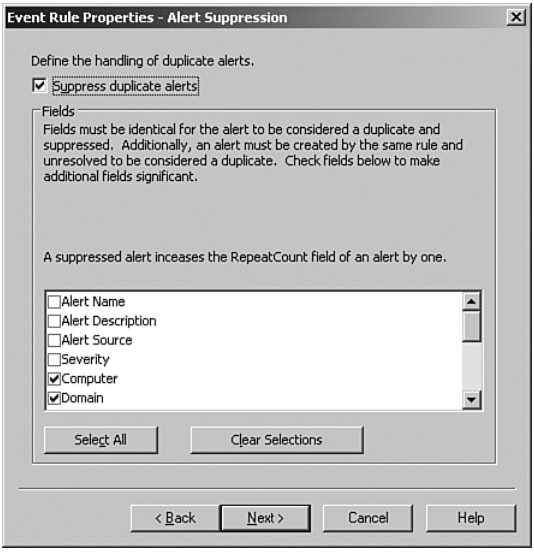


FIGURE 14.10 The Alert Suppression screen of an event rule.

6. The Responses Event Rule Properties screen includes the potential responses for the rule. This screen specifies the action (response) that will take place if the event occurs. The responses available depend on whether the rule is configured to

generate an alert. If you configured the rule to generate an alert, the possible responses are shown in Figure 14.11.

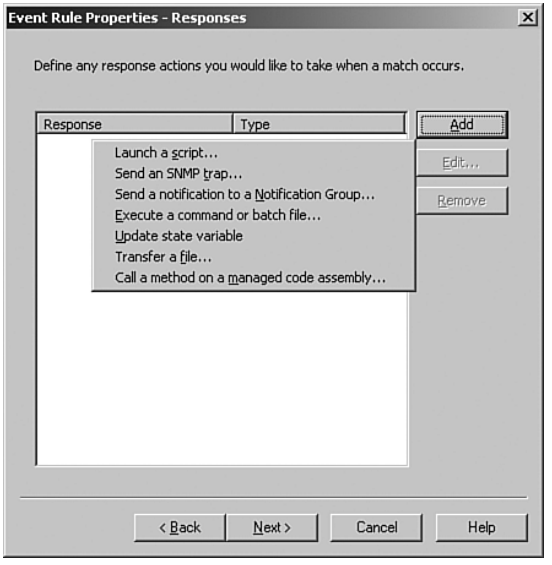


FIGURE 14.11 The Responses screen of an event rule that generates an alert.

If the event rule you are creating does not generate an alert, the list of responses is decreased (the options to Send an SMTP Trap or Send a Notification to a Notification Group are removed), as shown in Figure 14.12.

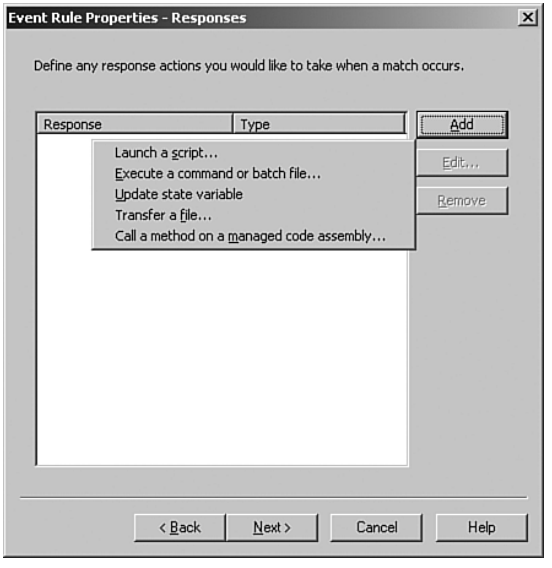


FIGURE 14.12 The Responses screen of an event rule that does not generate an alert.

We will review each of the seven response types (shown previously in Figure 14.11) in the "Response Types" section later in this chapter.

7. After configuring the responses, the next step of the wizard is to configure the Knowledge Base Event Rule properties. Figure 14.13 displays the Company Knowledge Base screen for the rule. The Company Knowledge Base is blank by default but as shown here can be used to provide documentation for the rule you are creating.

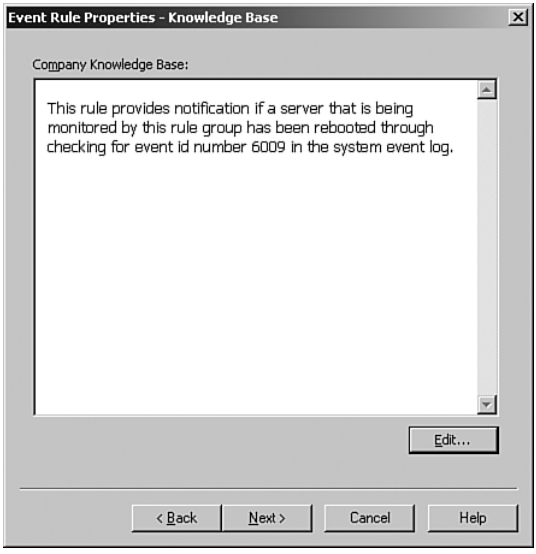


FIGURE 14.13 The Company Knowledge Base screen of an event rule.

Using the Company Knowledge Base

It is important to use the company knowledge base for documentation when creating rules within MOM. Examples of information often stored in the company knowledge base include why the rule exists, the rule's function, who created the rule, any manual actions required to resolve issues identified by the rule, and any other company-specific information related to the rule. The information specified on this page is added to the MOM database and associated with the created rule. When the rule generates an alert a link to the information is added on this screen.

8. The final step in the Rule Creation Wizard is naming the rule. Figure 14.14 shows the rule name screen for our example rule, which we have named Notification of Reboot. A rule's Globally Unique Identifier (GUID) is created as part of the rule creation process. The GUID can be helpful when attempting to track down where an alert originated or finding events using large amounts of space within the MOM database. On this screen you can also enable/disable the rule or create an override for the rule, which we discuss in the next section of this chapter.

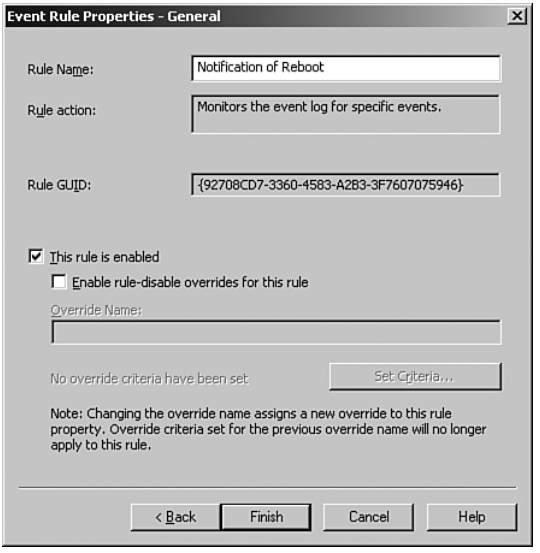


FIGURE 14.14 Naming the event rule.

Overrides MOM can use overrides to force a rule to be disabled for a specific computer or group of computers, while leaving it enabled for all remaining computers. (Performance rules also use MOM overrides to provide different thresholds; we discuss this later in the "Performance Thresholds" section of this chapter.) Conversely, you can also disable a rule and then create an override enabling it for a specific computer or group of computers. Figure 14.15 shows a sample override criteria screen.

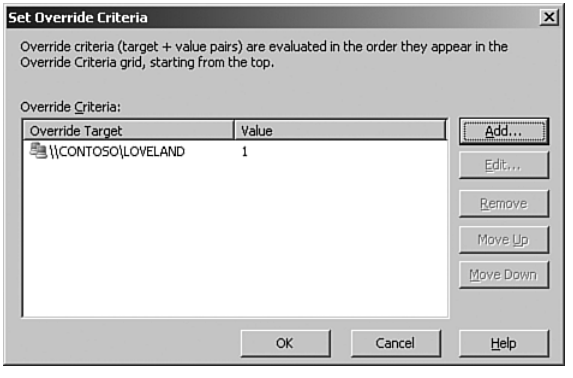


FIGURE 14.15 The Set Override Criteria screen in an event rule.

Overrides Without MOM 2005 SP1

There were significant issues with overrides prior to MOM 2005 Service Pack 1. If you plan to use overrides, you should upgrade to MOM 2005 SP1 prior to attempting to create overrides within your environment. Details on the primary issues (and a pre-SP1 hotfix) are available at http://support.microsoft.com/kb/898466/.

Using Overrides for Exceptions At times you may want to make exceptions to a given rule for a particular computer or group. There are also some built-in problems with the performance counters related to multiprocessor and hyperthreaded systems, as pointed out in the following note. Overrides can be used for disabling rules, setting different thresholds, and setting different script parameters based on a specific list of computers or computer groups.

Flaw in the % Processor Time Counter with Multiprocessor Systems

The Process performance object has a % Processor Time counter which has the following prosaic description:

% Processor Time is the percentage of elapsed time during which all process threads used the processor to execute instructions. An instruction is the basic unit of execution in a computer, a thread is the object that executes instructions, and a process is the object created when a program is run. Code executed to handle some hardware interrupts and trap conditions are included in this count.

In nontechnical language, the counter is supposed to be the percent of total processor time that the process is consuming. This measure works great for a single processor system, where the value will range from 0% to 100%. However, for multiprocessor and hyperthreaded systems, the value of the counter will range from 0% to 100% x Number of Processors. In the case of a two-processor system, the high-end value of the counter would be 200%. For a four-processor system, the high-end value of the counter would be 400%.

The result is that rules will trigger incorrectly for multiprocessor systems. If a threshold rule is created to trigger at 90%, it will trigger at 90% of total processor utilization on a single-processor system, 45% of total processor utilization on a dual-processor system, 22.5% of total processor utilization on a quad-processor system, and so on. Due to this underlying problem, a number of MOM 2005 rules ship disabled.

Overrides provide a way of automatically adjusting a given rule.

To allow an automatic adjustment to the trigger values based on the number of processors in the system, we will gather the information, group the computers, and configure overrides to properly set the thresholds.

The first step is to capture the number of processors in a system. This is the total number of processors that the operating system sees, taking hyperthreaded systems into account. For example, if a managed computer has two physical processors and supports hyperthreading, the number of processors seen by the operating system would be four. We can

use the computer attribute to capture the number of processors. The following are the steps to collect this information:

1. Launch the Administrator console.
2. Navigate to Management Packs \ Computer Attributes.
3. Right-click on Computer Attributes and select Create Computer Attribute.
4. You can select to base the attribute collection on a registry value or key, but select Registry Value in this case.
5. Click Next.
6. Type in **SYSTEM\CurrentControlSet\Control\Session Manager\Environment\ NUMBER_OF_PROCESSORS** for the path to the registry value.
7. Alternatively, you could browse for the value on the local or remote computer, which can be a useful timesaver to finding the correct registry information.
8. Click Next.
9. Set the attribute to retrieve the registry value and convert to integer. Click Next.
10. Enter the name **Number of Processors** and click Finish.

Now that we have a way of determining the number of processors in a computer, we want to use that to place the computers into computer groups that represent the number of processors. This allows us to set threshold criteria appropriate to each group and thus the number of processors in the managed computer. To create the groups follow these steps:

1. In the Administrator console, navigate to Management Packs \ Computer Groups.
2. Right-click on the Computer Groups node and select Create Computer Group.
3. Click Next past the wizard introduction.
4. Enter **One Processor Systems** for the name and click Next.
5. Click Next to move past the included subgroups screen.
6. Click Next to bypass the included computers list.
7. Click Next to skip the excluded computers list.
8. Check the Search for Computers Using All Criteria Specified Below and check all the selection boxes (servers, client, domain controllers, unknown, cluster virtual servers) under the text that says Include Computers That Are: on the Search for Computers screen.
9. Select the With Any Name radio button and click Next.
10. Select Specify a Formula for the Computer Group radio button.

11. Enter the following formula in the formula box:

    AttributeValue(Number of Processors)=1

    This will match the value of the attribute to a single processor system.

12. Click Next to accept the formula.
13. Select The Worst State of Any Member Computer or Subgroup radio button and click Next.
14. Review the setting in the confirmation window and click Next.
15. Click Finish to complete the setup.

Repeat the preceding steps to create computer groups named Two Processor Systems and Four Processor Systems, with the appropriate value in the formula for the number of processors. Table 14.1 lists a summary of the computer groups.

TABLE 14.1 Multiprocessor Computer Groups and Formulas

Computer Group Name	Formula
One Processor Systems	AttributeValue(Number of Processors)=1
Two Processor Systems	AttributeValue(Number of Processors)=2
Four Processor Systems	AttributeValue(Number of Processors)=4

Now that we have computer groups that correctly group the managed computers by the number of processors, we will configure a threshold rule to properly trigger for multi-processor systems. Follow these steps:

1. From the Administrator console, select a rule with a threshold value that depends on the processor utilization.
2. Click on the Threshold tab.
3. Check the Enable Threshold Overrides for This Rule box.
4. Click on the Set Criteria button.
5. Click the Add button to add an override criteria.
6. Click on the selection button next to the Target field and select Computer Group.
7. Select the Two Processor Systems computer group.
8. Enter **10** in the Value field to trigger at 5% of the total processor time for dual processor systems.
9. Click OK.
10. Click the Add button to add an override criteria.
11. Click on the selection button next to the Target field and select Computer Group.

12. Select the Four Processor Systems computer group.
13. Enter **20** in the Value field to trigger at 5% of the total processor time for quad processor systems.
14. Click OK.
15. Click OK to set the override criteria for the rule.
16. Click OK to save the modified rule.
17. Commit the configuration changes and wait for it to propagate.

The rule will now behave properly for dual and quad processor systems, triggering at 5% of the total processor utilization. This override will have to be set for each rule where you want the trigger to scale appropriately, though the computer attribute and computer groups are reusable.

Notice that we did not have to add an override criteria for the single processor managed computers because that is the default for the rule. In addition, we should do this for any rule that generates an error alert when the processor utilization goes above 50%. Of course, the thresholds will be different (100% for dual processors and 200% for quad processors). Table 14.2 lists the triggers and corresponding values for the computer groups.

TABLE 14.2 Computer Group, Triggers, and Corresponding Values

Computer Group	Trigger Utilization	Threshold Value	Override
One Processor Systems	5%	5	No
Two Processor Systems	5%	10	Yes
Four Processor Systems	5%	20	Yes
One Processor Systems	50%	50	No
Two Processor Systems	50%	100	Yes
Four Processor Systems	50%	200	Yes

Disabling Rules

The rules in MOM 2005 are designed to provide information for managing and monitoring your environment. However, you may find that there are alerts that are not relevant for your environment, in which case you can disable the underlying rule generating the alert.

To disable the underlying rule, open the Operator console and in the Alerts view select the alert in question. From here you can find the location of the rule in the bottom-right corner of the alert details, as illustrated in Figure 14.16.

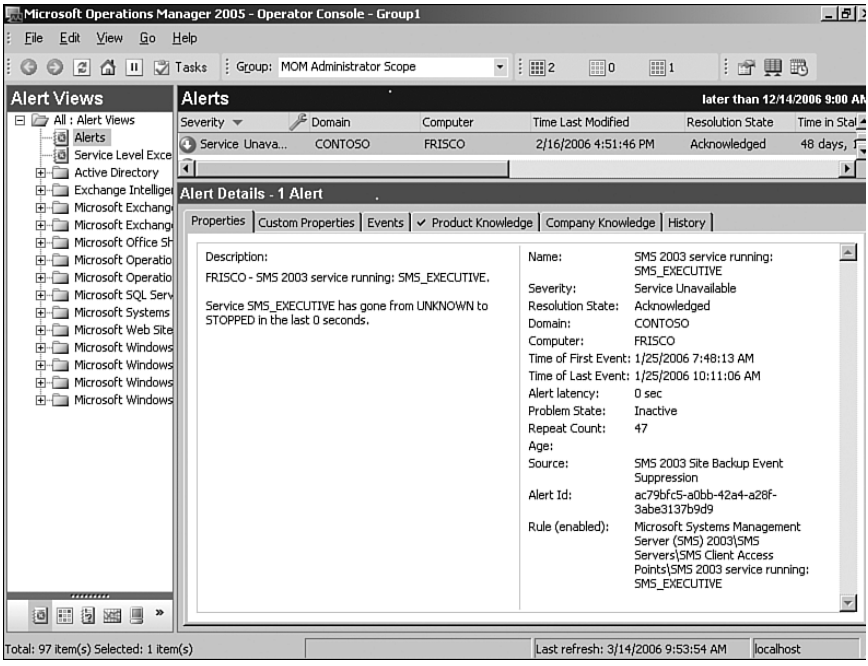


FIGURE 14.16 Identifying the underlying rule in an alert.

To disable the rule use the Administrator console and navigate to the path specified. Right-click on the rule and go to the properties page to uncheck the This Rule Is Enabled check box. Commit configuration changes to have your changes immediately applied.

Impact of Disabling a Rule

Disabling a rule disables it for all managed systems to which the rule had previously applied.

Disabling Rules

You can also disable a rule from within the Operator console. Right-click on the rule details and choose Disable Rule as shown in Figure 14.17.

Response Types

The sixth step of the Create Event Rule procedure (previously discussed in the "Alert on or Respond to Event" section of this chapter) displayed the Responses Event Rules properties screen, allowing us to specify response(s) to the rule. As we saw, MOM can take multiple actions as a result of a rule. The possible responses are as follows:

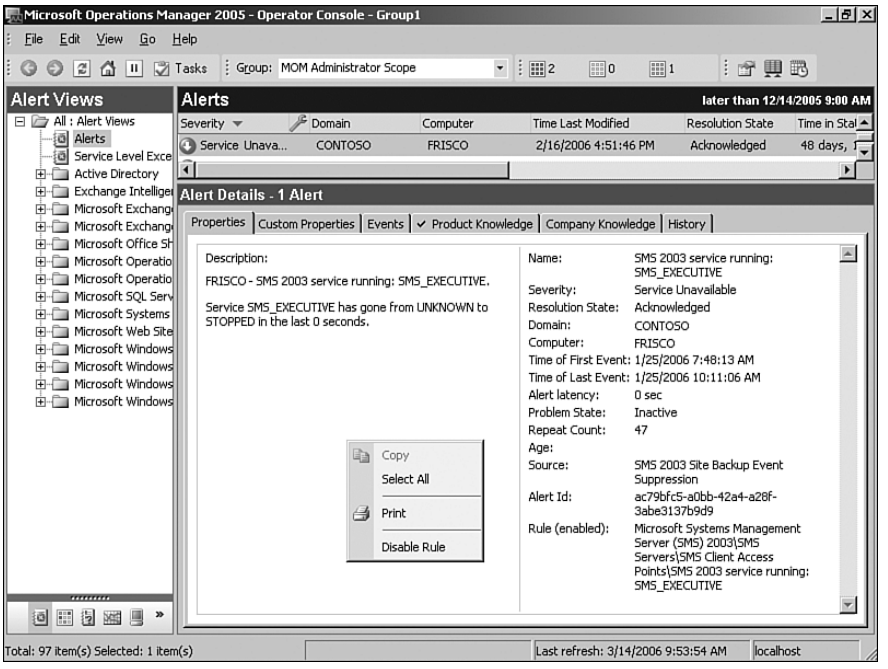


FIGURE 14.17 Disabling the rule within the Operator console.

- Launch a script—This response is used to launch any of the scripts available within MOM. The scripts available are shown within the Administrator console under Management Packs \ Scripts. Scripts can be run on either the managed computer or the management server.
- Send an SNMP trap—Generates a trap either locally on the agent or centrally on the management server. This type of a response is often used to send SNMP traps to other management consoles such as BMC Patrol, HP OpenView, Tivoli, and so on.
- Send a notification to a notification group—This response sends a notification to one of the notification groups defined within the Administrator console under Management Packs \ Notification \ Notification Groups. We discuss notification groups in Chapter 8, "Post-Installation Tasks."
- Execute a command or batch file—This calls a shell using cmd.exe on either the agent computer or the management server, which can be used to run Operating Systems commands (such as a `NET SEND`) or a batch file. Any batch file or command that is run must exist in the system path or the MOM agent installation folder, which by default is located at *%ProgramFiles%*\Microsoft Operations Manager 2005.
- Update a state variable—State variables are global variables stored on the management server. Using this response allows you to update the content of a state variable (increment, decrement, set value to a property, set value to text, set value to a number, or store the last *N* occurrences).

- Transfer a file—The file transfer response allows you to download or upload files using Background Intelligent Transfer Services (BITS). For example, the Baseline Security Analyzer (MBSA) Management Pack uses this functionality to download the MsSecure.cab file from the Microsoft website.
- Call a method on a managed code assembly—This response (Configure .NET Framework Response) provides the ability to call a method on a managed code assembly.

Filter Event (Pre-Filter)

Another type of event rule is the Filter Event rule, which allows you to stop an event from being inserted into the MOM database but allows a response to occur. This type of rule is useful in conserving space within the MOM database.

As shown previously in Figure 14.3, you can create this type of rule by selecting the Filter Event option. Choosing this option initiates a wizard to create a filter event. Most of the information required is similar to what was required when creating an event rule (specifying the provider, event criteria, and scheduling information). To provide an example filter event we will check the security log for event ID number 517, which indicates that the System event log cleared.

We follow the same steps as before to create an event rule (this time specifying the security event log, event ID 517). The wizard then asks you to specify the filtering action, shown in Figure 14.18.

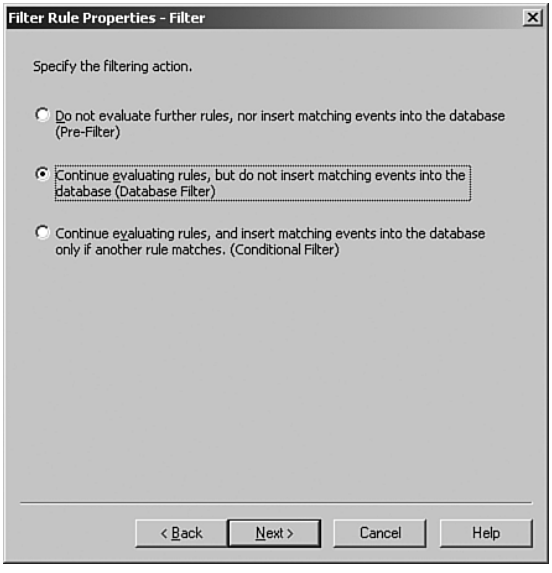


FIGURE 14.18 The filter action criteria screen in the Filter Rule Creation Wizard.

Three filter capabilities are listed:

- Pre-Filter—This option does not insert the event into the database and does not evaluate any other potential rules that match the criteria from the event. A pre-filter rule does not have any available responses. Pre-filter rules are supported with MOM 2005 but will not be created or supported in the future by Microsoft and are not included in new versions of Microsoft management packs. *We recommend that you not use pre-filter rules to avoid potential upgrade issues as new versions of Operations Manager become available.*
- Database Filter—This option does not insert the event into the database but evaluates any other potential rules that match the criteria from the event. This filter allows responses to be carried out (such as sending a notification to a notification group), but it cannot generate an alert.
- Conditional Filter—This filter inserts the event data into the database only if another rule (or multiple rules) matches the criteria of the event. This filter also allows responses to be carried out but does not generate an alert.

Using Filters

Why would we want to use these filters and how would they work? Let's take our example of the 517 event, which indicates a cleared event log. We created a filter rule with a Security event ID of 517 as its criteria. We add a pre-filter. The result: MOM does not insert the event into the MOM database and does not process any other rules looking for the same event ID number, effectively ignoring/pre-filtering any rules with this event ID.

Now we take the same filter rule and apply a database filter. The result: MOM does not insert the event into the database, but it does process other rules looking for the same ID.

Finally, we take the same filter rule and apply a conditional filter. The result: MOM writes the event to the MOM database. If another rule is looking for the same event ID number it allows that rule to process.

Detect Missing Event (Missing)

The Detect Missing Event rule is a powerful but often overlooked feature in MOM 2005. Unlike other rules within MOM, this one notifies you when an event has *not* occurred.

This rule type is often used to monitor items such as backups. In the case of a successful backup, you can log an event to the event log when it completes. If the event does not occur within the time specified, the backup probably did not work. The Detect Missing Event allows you to identify this condition and generate an alert.

As shown in Figure 14.3, you can create this type of rule by selecting the Detect Missing Event option. Choosing this option initiates a wizard that creates a rule to detect a missing event. This time we will choose the Application provider and event criteria (because we have already used the system and security logs). We will set the criteria to look for event ID 8019, which indicates the successful completion of the NTBackup

process. On the scheduling screen, we must specify the time range when we would expect the event to be generated and the day(s) of the week the event should occur. As with the event rule, you can also generate an alert and specify responses. Figure 14.6 and 14.7 gave examples of how to configure the Schedule screen.

Consolidate Similar Events (Consolidation)

The Consolidate Similar Events rule is used to group matching events into a single event stored in the MOM database while tracking the number of occurrences of the event (the repeat count) within a specific period of time. This type of rule generates an alert when an event occurs a specific number of times within a given time period.

Using Consolidate Similar Events Rules

A good example of where to use the Consolidate Similar Events rule would be to track failed logons over a period of time, helping to determine failed logon trends.

As shown in Figure 14.3, you can create this rule type by selecting the Consolidate Similar Events option. This option initiates a wizard to create a consolidation rule.

Most of the steps are similar to those we reviewed when creating an event rule (specify the provider, event criteria, scheduling information). To provide an example consolidation rule we will check the security log for event ID 517, as we previously did with the original event rule creation. The additional screen provided for this rule type is the Consolidation Rule Properties screen displayed in Figure 14.19.

In this screen, you specify which fields the event must match to qualify to be consolidated. You also specify the consolidation period (in seconds). This rule type does not allow an alert or response to be defined, but it can be combined with an event rule. We discuss this further in the "Combining Rules" section later in this chapter.

Collect Specific Events

The last of the five event rule types is the Event Collection rule. The Event Collection rule is used to collect events with specific event parameters in their criteria. This type of rule is often used to collect SNMP information or gather Internet Information Server (IIS) log information.

As shown in Figure 14.3, you create this type of a rule by selecting the Collect Specific Events option. The collection rule is used to store event information within the MOM database but does not generate an alert or perform a response. Most of the selection criteria are similar to the steps we have reviewed when creating an event rule (specifying the provider, event criteria, scheduling information). The unique screen for this rule type is the Parameter Storage Collection Rule Properties screen, shown in Figure 14.20. An example of this rule type is in the Windows Base OS (Server) Management Pack when it finds events from event log source with an event ID of 6006. If an event matches these criteria, the rule does not store event parameter information. This particular rule is found under Management Packs \ Microsoft Windows Servers Base Operating System \ Windows 2003 \ Reliability \ Events \ System Stopped: The computer has cleanly shut down and is no longer available.

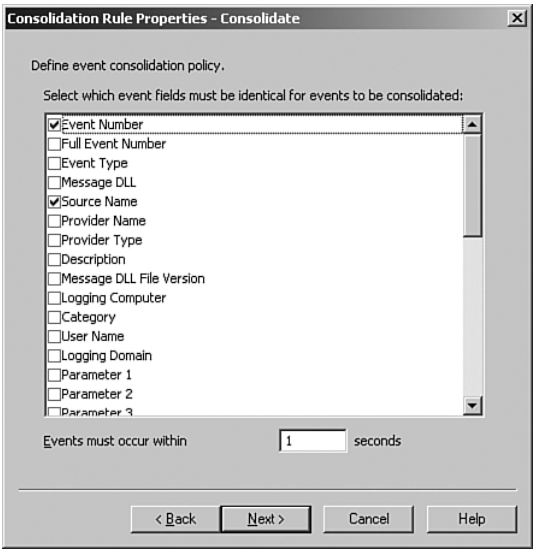


FIGURE 14.19 The Consolidation screen in the Consolidation Rule Creation Wizard.

When collecting the event three options are available: Store All Event Parameters, Store These Event Parameters, or Store No Event Parameters.

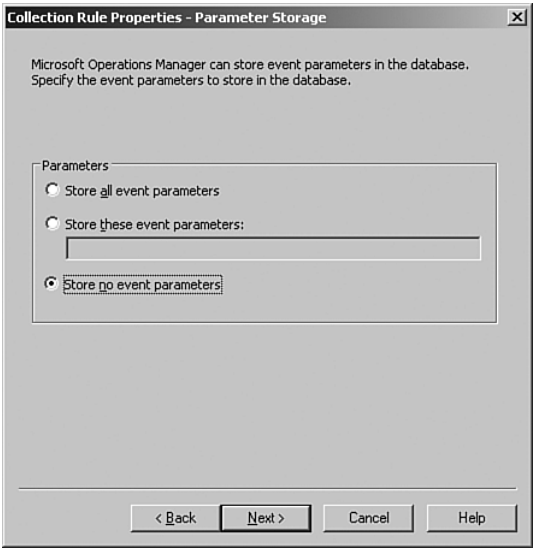


FIGURE 14.20 The Parameter Storage Screen in the Event Collection Creation Wizard.

Using Collect Specific Events Rules

The Collect Specific Events rule type is helpful when setting up event rules using specific event parameters within their criteria. For example, the IIS log contains several parameters. You can use this rule type to create a rule to collect the IIS log entries and store all the event parameters. In the MOM Operator console, you can then see which values in the IIS logs correspond to what event parameters. The result is a way to look up event rules and specify the parameters and values that you are looking for in the IIS log.

Combining Rules

In some circumstances it can be beneficial to use a combination of event rules. An example of this is combining the generation of an alert when the repeat count of an event (from a consolidation rule) goes beyond a value you specified. To accomplish this you would define at least two rules:

1. Create a consolidation rule that keeps the count of the event over the specified period of time using a specific ID as its event criteria.
2. The second rule provides an alert or responds to the event with the same event criteria. For this rule, you would also add the repeat count of the event, within the advanced criteria.

For our example we will monitor events within the application log created by a custom-built application called, logically enough, CustApp01. For our example (shown in Figure 14.21), we check for event ID 242 from the source of CustApp01 with a repeat count of greater than 1.

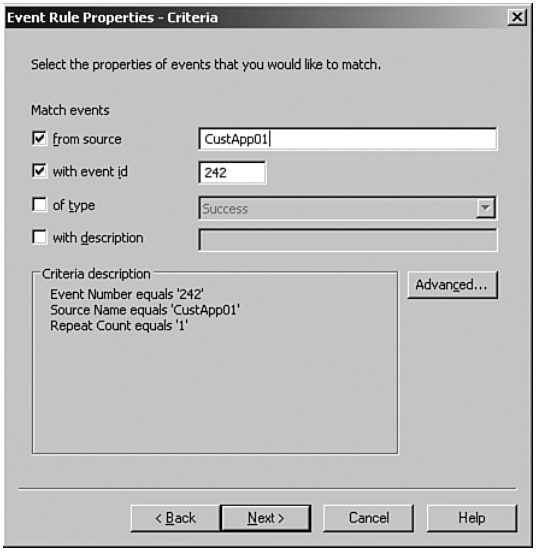


FIGURE 14.21 Specifying an event repeat count based on a consolidation rule.

Specifying the Occurrences of an Event

The first occurrence of an event creates a repeat count of zero, the second time that the event occurs it updates the repeat count to one, the third time it occurs it updates the count to two, and so on.

Our custom application will require at least three occurrences of the event in the time frame we specified within the consolidation period (created in the consolidation rule). An interesting aspect of how MOM works is that the alert is not generated until the end of the consolidation period. Therefore, if you set a repeat counter greater than one and a consolidation period of four hours, if you receive three occurrences of event ID 242 within the first few minutes of the consolidation period it still would not notify you until the 4-hour period is over.

Combining Event Rules

Combining rules can quickly become complicated when creating and maintaining the rules. Be sure to test the combinations of rules in detail prior to deploying them within a production environment.

Performance Rules

The next rule type we will discuss are performance rules. *Performance rules* provide MOM with the capability to sample and compare performance counters from either Windows Performance counters or WMI Numeric Events. The two major types of performance rules are the Sample Performance Data Type and Compare Performance Data Type. The various management packs from Microsoft already have rules that sample and compare data for most standard performance metrics, so in discussing performance rules we will investigate existing rules rather than create new rules.

Sample Performance Data

The MOM Sample Performance Data Type rule samples performance data and inserts it into the MOM database for analysis and trending. The performance information can be viewed in the Operations console within Performance Views. The data is available for trending information after it is transferred to the MOM reporting database. To look at the Sample Performance Data rule type, we will look at an Exchange 2003 rule that monitors SMTP submissions. This rule is the SMTP: Total Message Submitted and is located under Management Packs \ Rule Groups \ Microsoft Exchange Server \ Exchange 2003 \ Performance Counter Logging Rules \ Exchange Utilization and Performance \ SMTP Utilization. This rule monitors the number of SMTP messages submitted within a 15-minute time frame.

To create a sample performance rule, browse to our RuleTesting rule group, which we created earlier in this chapter. Right-click on Performance Rules and select the Sample Performance Data (measuring) option to initiate a wizard displaying the Provider screen, shown in Figure 14.22.

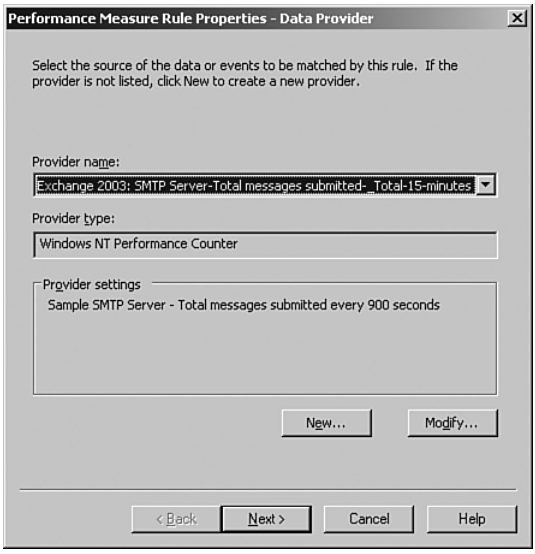


FIGURE 14.22 The Provider screen in the Performance Rule Creation Wizard.

The Provider screen allows you to select a predefined provider or create a new provider. The performance providers in MOM request a specific instance of a specific counter at a given interval. In this case, we will use a rule from the Exchange Server 2003 Management Pack. After we specify the provider name and type, we continue to the Schedule, Response, and Company Knowledge screens; then we name the rule we are creating. The Response screen is limited to the five event rules response options, which we previously discussed in the "Event Rules" section of this chapter.

Compare Performance Data

The Compare Performance Data rule type gives you a method to evaluate a counter (or the average of previous counters) against a threshold you define. This type of rule also allows you to generate an alert based on the value of the data. For example, the Exchange management pack uses this rule type to monitor disk read and write latencies. The rules that check disk read and write latencies for Exchange are located under Microsoft Exchange Server \ Exchange 2003 \ Health Monitoring and Performance Thresholds \ Server Performance Thresholds. The rules are Disk Read Latencies > 50 msec and Disk Write Latencies > 50 msec (the latter of which is disabled by default). If we check the properties of the rule on the Threshold tab, we see that the threshold is compared when the average taken over 10 samples has a value greater than .05 (50 msec) as shown in Figure 14.23.

The Threshold screen provides a method to compare the sampled value, the averages in the values over a number of samples, or the change in value over a number of samples. These options provide a way to look for trends or averages rather than using a single sample, which may be impacted by a small data spike. For example, it is far more useful to know that the disk latency is > 50 milliseconds (msec) over a large number of samples

versus knowing that it spiked with a single sample. The second set of options in this screen compares the sample and can alert when the sample is greater than or less than the specified value. The third option listed is Always, which matches regardless of the content of the sample. As with other rule types you can also define overrides for specific computers or groups of computers.

Always Matching in the Compare Performance Data Rule

Why would you want to alert regardless of the value of the data? The Always match is used when you are defining a state alert. A state alert represents the current health of the computer(s) shown by color as green, yellow, or red. We discuss state alerts in the "Alerts and State Management" section later in this chapter.

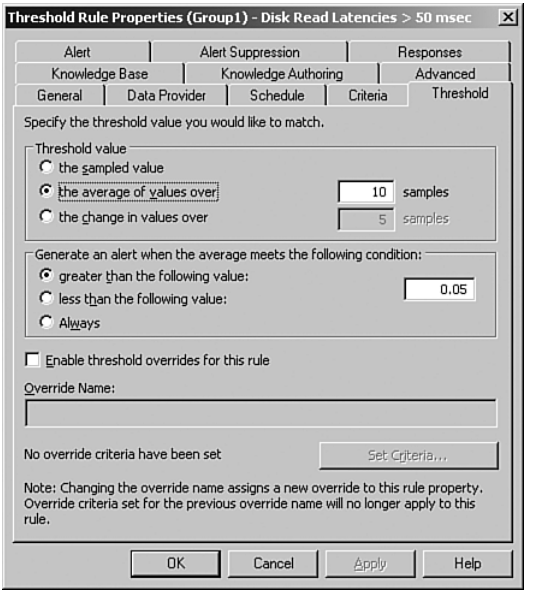


FIGURE 14.23 The Threshold screen in a Compare Performance Data rule.

You can also configure an alert as part of the properties of your threshold rule. Figure 14.24 is similar to the Alert screen for event rules.

The steps to create a Compare Performance Data rule are the same as that for a Sample Performance Data rule, but when choosing the type of performance rule choose the Compare Performance Data (Threshold) rule. We utilize a criteria screen for this type of rule, as shown in Figure 14.25.

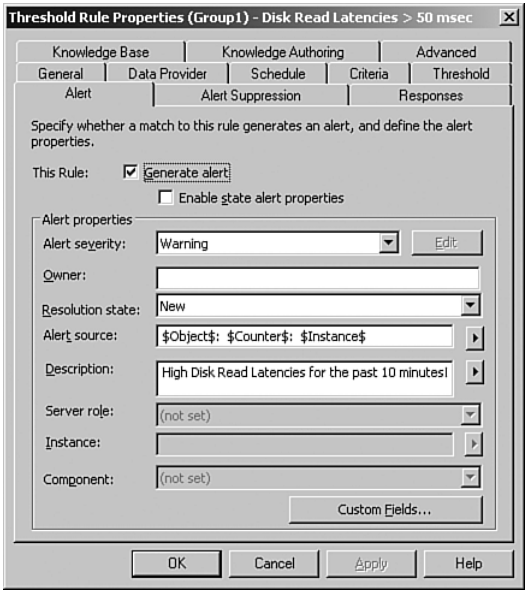


FIGURE 14.24 The Alert screen in a Compare Performance Data rule.

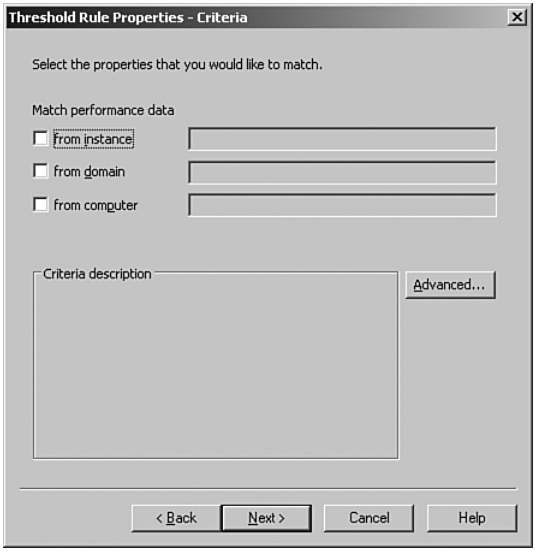


FIGURE 14.25 The Criteria screen in a Compare Performance Data rule.

The Criteria screen provides a method to restrict the criteria based on instance, domain, or computer. By using advanced criteria, you can also specify the object and/or a counter.

To create a performance rule, browse to the RuleTesting rule group created earlier in this chapter. Right-click on Performance Rules; then select the Compare Performance Data (Measuring) option, which initiates a wizard that displays the Provider screen. The wizard goes through the various common screens discussed in the "Event Rules" section of this chapter (scheduling, alert generation, suppress duplicate alerts, responses, knowledge base, and rule naming) with the only custom screens being the Threshold screen shown in Figure 14.23 and the Criteria screen shown in Figure 14.25.

Alerts

Alerts are used by MOM to provide notification and tracking, or to document a condition detected by MOM. As we have discussed, alerts can be generated from event rules (refer to Figure 14.9) or performance threshold rules (refer to Figure 14.24). They can also be generated by scripts, which can generate or modify alerts.

You can forward alerts to another MOM management group using the MOM-to-MOM Product Connector (discussed in Chapter 19, "Interoperability") or other third-party monitoring systems or problem tracking systems. Based on your design parameters, alerts may be designated as the primary tracking and documentation mechanism for your operations staff.

Alert Rules

The third and final type of rule within MOM 2005 is the alert rule. *Alert rules* act on alerts generated from event rules, performance rules, script-generated alerts, or alerts forwarded into MOM. You can use alert rules to perform actions such as sending notifications to notification groups based on characteristics of the alert (severity, description, and attributes). You can also use alert rules to provide a single notification response for all alerts matching the criteria that you specify (rather than configuring individual events to provide notification).

The process to create an alert rule is similar to that of an event or performance rule. For our example, we will browse to our testing rule group created earlier in this chapter (located under Management Packs \ Rule Groups \ RuleTesting \ Alert Rules). Right-click on Alert Rules in the Administrator console and select Create Alert Rule. The Alert Rule Wizard's first screen is shown with the Alert Criteria screen displayed in Figure 14.26.

This screen is designed to provide a way to bind the rule to specific alerts. In addition to the alert source and severity, a number of other fields are available within the Advanced criteria selection (Alert Description, Alert Name, Computer, CustomField1-5, Domain, Owner, Resolution State, and Time). The Only Match Alerts Generated by Rules in the Following Group check box provides a way to have the rule apply only to alerts generated by the rule group you identify. If you do not check this box, the alert rule applies to all rules in the MOM database that generate alerts—so it is highly recommended to check this box and select the appropriate rule group.

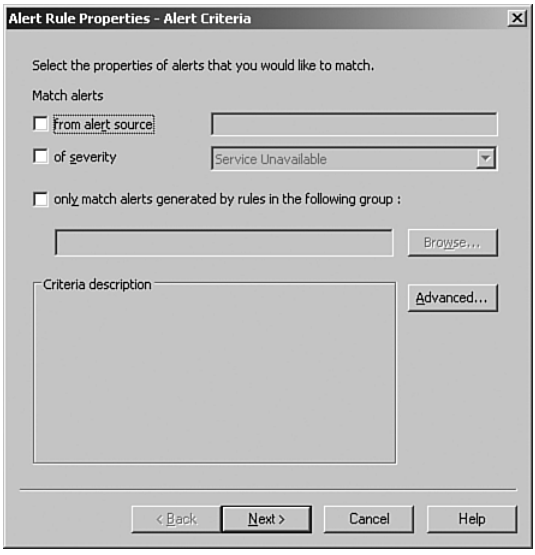


FIGURE 14.26 The Criteria screen in an alert rule.

Alert Rules

An alert rule applies only to the specific rule group. An alert does not apply to any subgroups below the specified rule group.

The remainder of the screens in this wizard were discussed earlier in the chapter (schedule, responses, knowledge base, and rule naming). On the Responses page all seven responses are available. These responses were previously discussed in the "Event Rules" section of this chapter.

You may be asking yourself: Why create an alert rule if I can just do this using my event rules? That is a valid question, and here is the primary answer: You can use an alert rule to group together similar alerts for notification from the alert rule, instead of creating individual alerts within each event rule. This is a far more efficient option when you are using multiple event type rules that utilize alerts.

Generating Alerts

We have discussed alerts from a more general perspective within the event and performance rule types. Figure 14.27 shows an Alert screen used when creating an event type rule. We will review the fields on this screen to provide more detail.

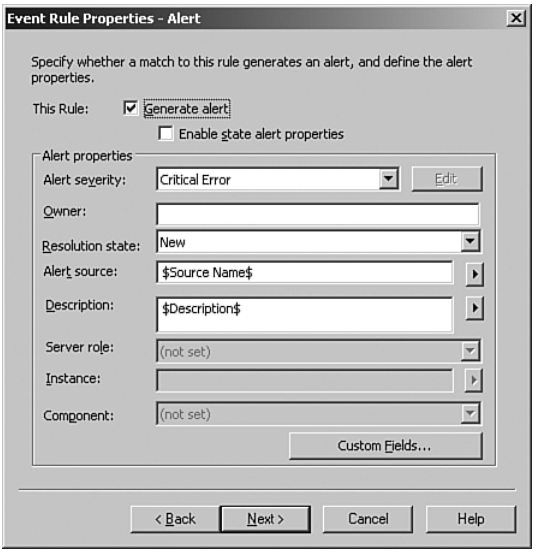


FIGURE 14.27 A sample alert within MOM 2005.

The screen has several fields you can customize. The fields and their descriptions are as follows:

- Generate Alert—This check box activates the remainder of this screen.
- Enable State Alert Properties—This check box activates the Edit button on this screen, providing the ability to change alert severity conditions.
- Alert Severity—The following severities exist for an alert (in order of severity): Service Unavailable, Security Issue, Critical Error, Error, Warning, Information, and Success.
- Owner—The person or group responsible for resolving the alert.
- Resolution State—The initial state that an alert will exist in when created (typically set to New). The default options include New, Acknowledged, Level 1 through 4, and Resolved. These can be customized with the Administrator console at Administration \ Global Settings \ Alert Resolution States.
- Alert Source—This field identifies the system or application that generated the alert. This field defaults to the `$Source Name$` parameter of the event firing the rule.
- Description—This field provides additional information about the alert. This field defaults to the event description of `$Description$` but has options including: Category, Description, Event Type, First Time, Full Event Number, Last Time, Logging Computer, Logging Domain, Message DLL, Message DLL File Version, Parameters 1 through 25, Provider Name, Provider Type, Repeat Count, Source Computer, Source Domain, Source Name, Start Time, and User Name. This field is

typically used to generate emails or pages indicating details of the condition that MOM has detected.

- Custom Fields—Custom fields can be added to the alert to include other parameters that would be useful when providing details on the alert.

Figure 14.27 also includes several grayed-out fields:

- Server Role—This field (in addition to the Instance and Components fields) is activated when the Enable state alert properties check box is checked. (State management is discussed in the next section of this chapter.) The field specifies the role the server plays in regard to the alert. Examples of this include the MOM Agent or Exchange.
- Instance—Used to specify the instance of the alert. Examples are the source domain or provider name.
- Component—Specifies the component of the server role. For example, for Exchange the components are Databases, Mail Flow, Message Application Programming Interface (MAPI) Logon, Queues and Services.

The Alert That "Cried Wolf"

Let's say an in-house application generates event 242, indicating that the application encountered a problem and cannot continue. If the application is mission-critical and the problem must be resolved as quickly as possible, the severity should be set to Critical Error or Service Unavailable. You could contrast this with an alert indicating that a printer is out of paper (the printer is in the end-user area and often used to print personal documents). If you set the severity to Security Issue, your operations staff responds accordingly and takes this alert very seriously, only to find out that the printer ran out of paper when someone printed his child's science project. Future alerts generated as Security Issue may not be taken as seriously by the operations staff next time.

It is important to avoid alert overload with MOM 2005. To prevent generating unnecessary alerts you should tune the environment to alert on the minimum number of conditions that require an alert and provide an appropriate alert severity.

Alerts and State Management

State management is a core concept within MOM 2005. The state of a server is displayed in the Operator console to provide a graphical representation of the current "state" or health of the computers or computer groups within the monitored environment. State views are based on color and follow the analogy of a stoplight: Red indicates an error (stop), yellow indicates a warning (slow down or speed up depending on your interpretation of traffic laws), and green signifies things are good (go). State management in MOM builds on the concepts of roles and components. A *role* is a function that server(s) perform

(example roles include database server, domain controller, mail server, and web server). A *component* is a piece of that role being performed. For example, the Active Directory server role is broken into components of Client View, Replication Health, Server Health, and Service Health.

Management packs provide application-specific state views (such as Active Directory, Microsoft Exchange Server). These views show the color corresponding to the highest level of severity of alert for the computers making up that computer group or application. The current state shows the color (red, yellow, or green) corresponding to the highest severity of alert on the computers that comprise the computer group or application, which is the state being described. Figure 14.28 shows a State view in the MOM 2005 Operator console.

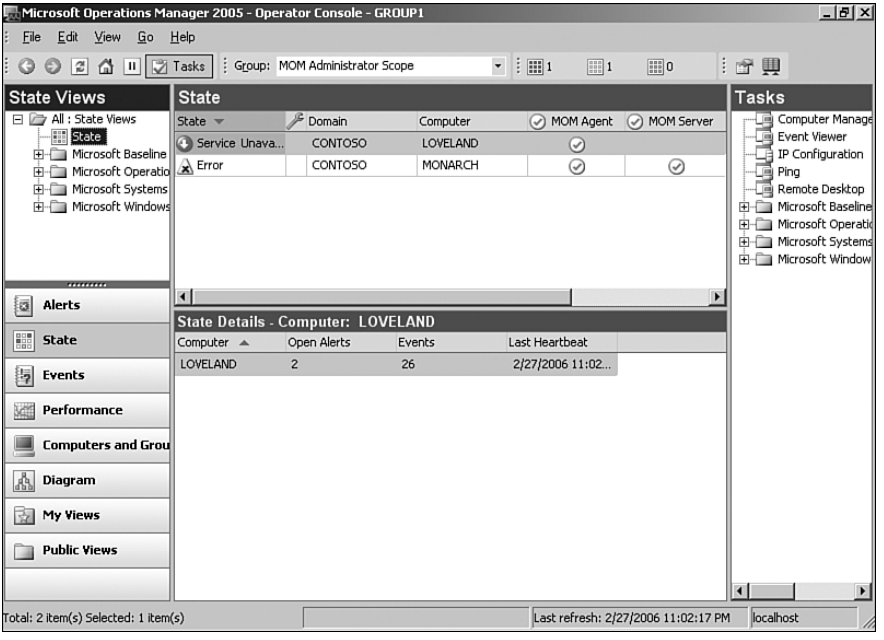


FIGURE 14.28 A sample State view in the MOM 2005 Operator console.

The severity of the alert directly affects the overall state of the application or server role shown within the Operator console. Notice that the total numbers (# Red, # Yellow, # Green) within the console reflects the highest severity alert for each server.

Alert Severities

When an alert is generated, you can use a formula to configure the alert. A formula gives you additional flexibility to set the alert severity based on the measured value. A formula can also set the alert severity to a "green" level of severity when the problem is corrected. Figure 14.29 shows an example of this.

The example shows a check of free disk space where the level of the alert depends on the percent of disk space use. If the percent of disk space used is greater than 90%, it is classified as a Critical Error; if the percent is greater than 50%, the alert is a (non-critical) Error; and if the percent of disk space used is not greater than 50%, it no longer represents an error condition. Thus, if the value is 60, the alert is set to Error, but if the value increases to 95 it becomes a Critical Error. Finally, if the value decreases to 40, the Alert is set to No Problem, which sets the problem state as Inactive.

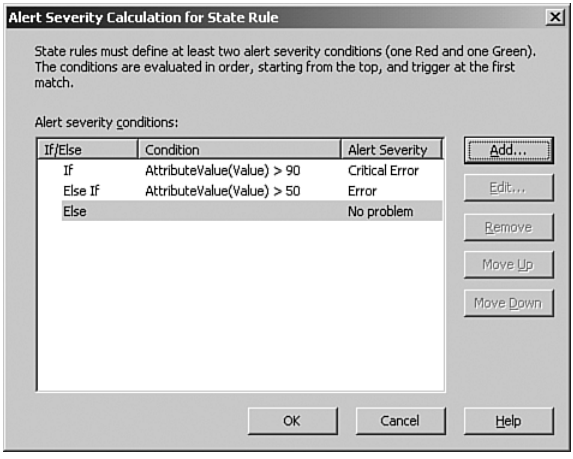


FIGURE 14.29 Calculating the alert severity for a state rule.

Defining State Properties

When using a formula for the state properties the last condition must always be an Else, No Problem.

Problem States

Problem states are used to calculate the state of an application, computer, or computer group and are visible within the Operator console. Problem states are the current state of an alert, which contributes to the overall state of the application, computer, or computer group. There are three problem states:

- Active—This is the problem state for a new alert. The active problem state is a state alert that is not resolved. One example of this would be when a service has stopped.
- Inactive—The alert has been resolved. In our example, this occurs when the service is restarted. When an alert is set to this problem state by default it is automatically resolved by MOM within an hour. This configuration can be changed within the Administrator console \ Global Settings \ Alert Resolution States on the Database Grooming tab.

- Investigate—This state is used for alerts that are not inherently state based. Nonstate-based alerts are put in the Investigate problem state by default.

State Management Documentation

More information about state management can be found in the MOM 2005 Management Pack Development Guide, available at http://go.microsoft.com/fwlink/?linkid=50020.

Alert Resolution States

A key component of an alert is its resolution state, which indicates the current state of an individual alert. As we discussed in the "Generating Alerts" section earlier in this chapter, the typical initial alert resolution state is set to New. Figure 14.30 shows the default resolution states in MOM 2005.

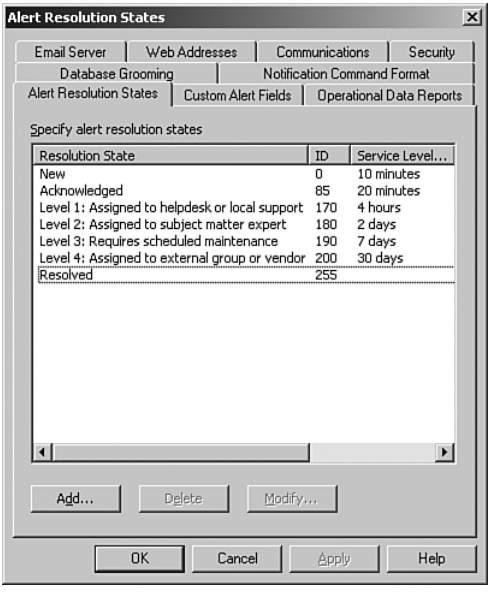


FIGURE 14.30 The alert resolution states from the MOM global settings.

The MOM-to-MOM Product Connector uses the resolution states to forward alerts to a higher tier management group within MOM. Details on product connectors are discussed in Chapter 19.

As shown in Figure 14.30, service level agreements (SLAs) are built into the resolution state. These resolution states have a maximum amount of time that an alert is expected to exist within that state. By default the maximum time an alert can be in the New state is

10 minutes and the maximum time an alert can be in the Acknowledged state is 20 minutes.

The resolution state of an alert can be changed in the MOM Operator console by right-clicking on the alert and selecting the Set Alert Resolution State to the New state. If an alert does not move to the next state within the time specified for the SLA the alert is then listed in the Service Level Exceptions alert view. Figure 14.31 shows an example of the Service Level Exception within the Operator console.

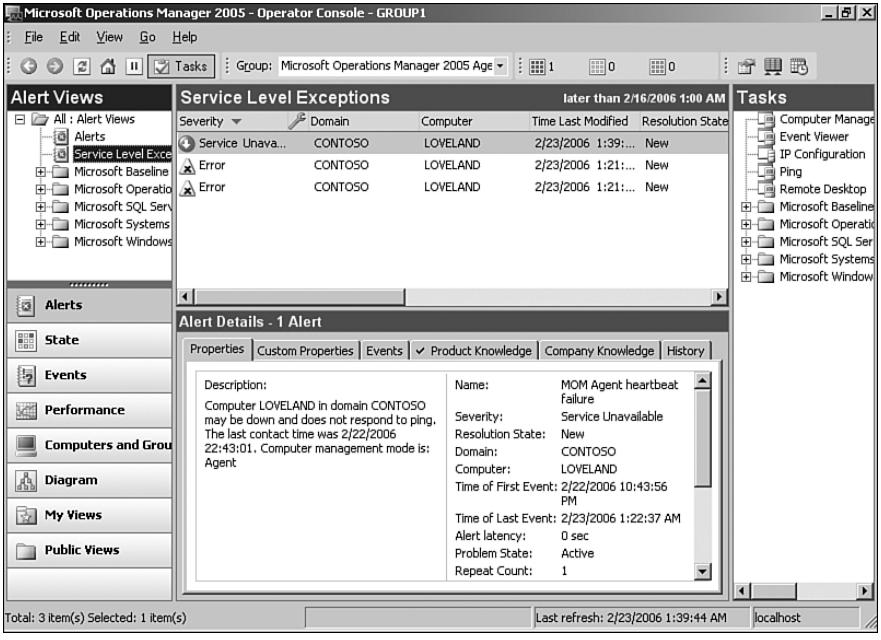


FIGURE 14.31 A service level exception displayed in the MOM 2005 Operator console.

The resolution states are customizable as discussed in the "Generating Alerts" section earlier in this chapter. You can update the existing states, create new states, or update the SLA information to meet the requirements of your company.

Enhancing Escalation Capabilities

As an example of how you can customize notifications, we are including a simple management pack (Escalation Notification) that provides rudimentary escalation alerting. This management pack runs a script that checks the operational database for alerts that match specific criteria, and if it finds the criteria, writes an event to the event log with the information. Additional rules in this management pack find the logged events and provide notification to the groups defined in the management pack.

For example, if an alert exists that has not been resolved within 120 minutes; a notification is sent to the EscalationLevel1 notification group. The escalation levels continue up to Level 5, which is utilized when the alert has not been resolved within

one week. If you have many unresolved alerts, this management pack may generate a significant number of notifications, so it should be first deployed into a properly tuned and tested environment.

When deploying this management pack you will need to add the management server into the Escalation Notification Server computer group and define members within the EscalationLevel1-5 notification groups.

The Escalation Notification Management Pack is on the CD included with this book.

At the Microsoft Management Summit (MMS) 2006 Microsoft released new escalation scripts. These scripts are available for download thanks to the crew at MOMResources.org at http://www.momresources.org/scripts-momadministration.shtml. The escalation scripts are called Notification Escalation – Scan Alerts and Notification Escalation – Set Delay.

The Life Cycle of an Alert

Let's put a perspective on how alerts work within MOM 2005 by walking through the life cycle of an alert:

1. The alert is generated. There are a number of ways that this may occur, which include being created by an event rule or a performance data rule, being generated by a script, or being forwarded from a lower-tier management group. Figure 14.32 shows an alert with an initial resolution state of New, and the problem state as Active (default conditions for this alert).

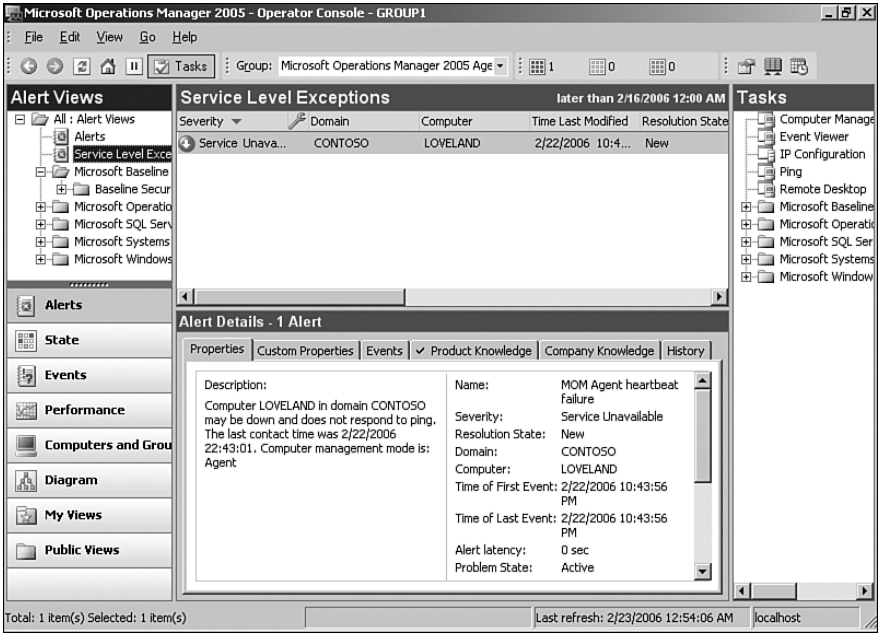


FIGURE 14.32 A new alert in the Operator console.

2. The alert is acknowledged by your operations staff, and the resolution state is changed to Acknowledged. In this case the state was manually changed, but the resolution state can also be changed by a script running as a response to the alert. Figure 14.33 shows the state as Acknowledged.

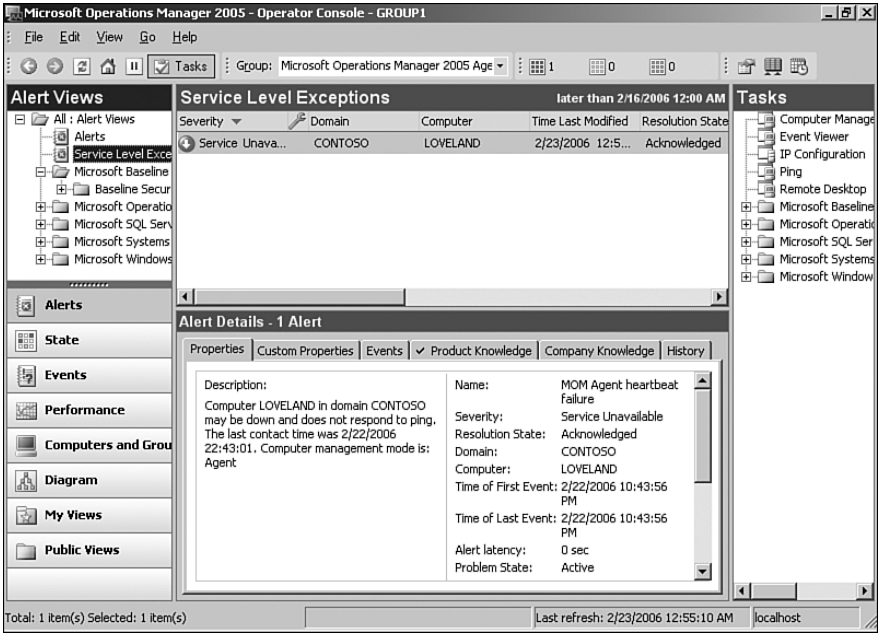


FIGURE 14.33 The alert is acknowledged.

3. Because this alert occurred outside business hours, the person on call (perhaps notified by MOM of the incident) connects from home using a Virtual Private Network (VPN) connection and takes appropriate steps to resolve the situation.

In this instance the alert is manually changed to Resolved, although the alert could also have a clearing event generated to automatically change the problem state to Inactive. After the status changes to Resolved it disappears from the view in the Operator console because the default view only displays unresolved alerts.

When the alert is changed to Resolved, the person performing the action can document details of the resolution as shown in Figures 14.34 and 14.35. This information is applied to the Alert history but is not carried forward the next time a rule generates an alert of the same type (and the data is also lost when the alert is groomed from the MOM database). A recommended approach in documenting this information is updating the company knowledge section of the rule that generates the alert because the information is not groomed out and will be available the next time this alert is generated.

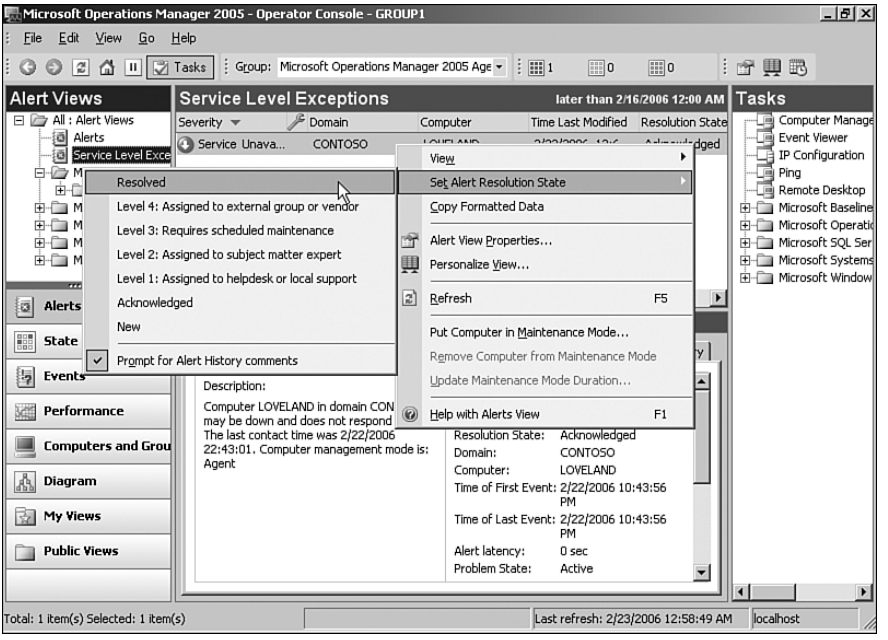


FIGURE 14.34 The option to update the alert history.

Figure 14.35 shows where the history can be updated.

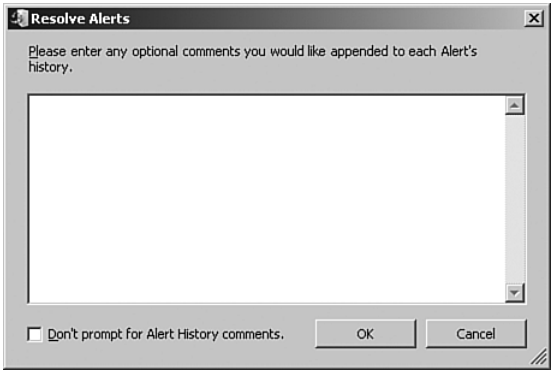


FIGURE 14.35 Updating the alert history.

Alerting in Real Life

The alert life cycle is a simple example. Many configurations can make this a more complicated workflow. Your company might have a problem-tracking system that documents problems and resolutions, or you could update the alert knowledge to include the trouble ticket number from your problem tracking system.

You could also have a tiered support structure where a Level 1 support team is initially assigned the issue. Several minutes later, the issue is escalated to Level 2, and so on. Each of these actions can be tracked in the MOM Operations console manually or automated with scripts.

The intent is for MOM to portray an accurate picture of the health of your organization. Your MOM implementation is successful when the alerts it generates represent real issues to address, rather than a myriad of untested and unverified alerts that are generated and ignored.

How to Get Rules Where You Need Them

Not all rule groups are created equal. Part of the beauty of MOM is its capability to put the right rules where they are needed without cluttering up systems with the wrong rules.

MOM determines what identifies a specific application and creates a list of systems that match; then MOM deploys the appropriate collection of rules to each system. In MOM-speak, we would say: MOM collects attributes and assigns systems to computer groups based on those attributes and then deploys rule groups to the computer groups. Figure 14.36 shows this four-step process. The process establishes a link from the specific configuration settings on a computer to the delivery of rules to that computer.

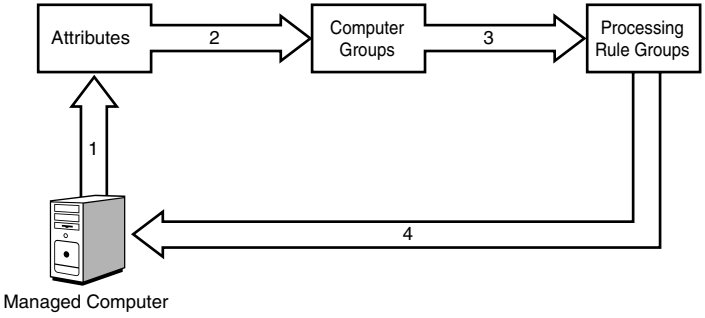


FIGURE 14.36 Delivering rules to computers.

As part of how we get rules where they are needed we need to discuss attributes, computer groups, and rule groups.

Attributes

Attributes are characteristics of systems, specifically registry keys or registry values. Attributes give you a way to identify what applications the systems have loaded, what versions they have installed, how they are configured, or anything else you can glean from the registry of a system. Attributes are collected during the nightly scan of managed computers.

Table 14.3 shows some examples of attributes collected by MOM by default. These attributes determine the existence and version of Exchange servers, as well as whether a managed computer is a DNS server.

TABLE 14.3 Sample Computer Attributes Collected by Default

Name	Description	Type	Registry Path	Value
MSExchange Server	Check for existence of the MSExchangeSA registry key to verify existence of full Exchange Server installed	Key	SYSTEM\CurrentControlSet\Services\MSExchangeSA	Check for Key
MSExchange Server Version	MSExchange Server Version as integer	Value	SOFTWARE\Microsoft\Exchange\setup\newestbuild	Retrieve Integer
Microsoft DNS Server	Detects if DNS service is installed	Value	SYSTEM\CurrentControlSet\Services\DNS\Start	Retrieve Integer

Approximately 45 different attributes are established by the various management packs that ship with MOM 2005. You can review the attributes in the Administrator console in the Management Packs \ Computer Attributes node.

Computer Groups

MOM uses computer groups to group computers that need to have the same rules delivered to them. This allows collections of rules to be created and delivered as a group to specific systems. You can also use computer groups to administratively assign control of the management environment. By associating console scopes with computer groups, you can restrict an individual user's permissions in the MOM consoles.

Computer groups can group computers by the following methods:

- Role, domain, and computer names—You can use the role, NetBIOS domain, and/or computer names to identify computers that should belong to a computer group. The roles can be Servers, Clients, Domain Controllers, and Cluster Virtual Servers. Wild card characters, regular expressions, and Boolean regular expressions can identify computers by domain and computer name.
- Computer attributes—Use computer attributes to dynamically select which computers should be part of the computer groups. This method is much more flexible because it can dynamically identify systems that have applications installed and deploy the rule to them.
- Including or excluding—You can also include or exclude a specific computer, which takes precedence over the dynamic methods. A good example of where you might need to include a computer is when managing computers in a DMZ (demilitarized zone) because the Action account would be unable to scan the registry and collect attributes of those computers.

Computer groups can group computers by attribute values to identify installed applications and services, but they can also group the computers by geographic boundaries, functional boundaries, or operations boundaries.

Working from our sample attributes (shown in the previous "Attributes" section) on Exchange as well as a few others, the corresponding computer group would be Microsoft Exchange Server 2003 Backend and would have the formula shown in Figure 14.37.

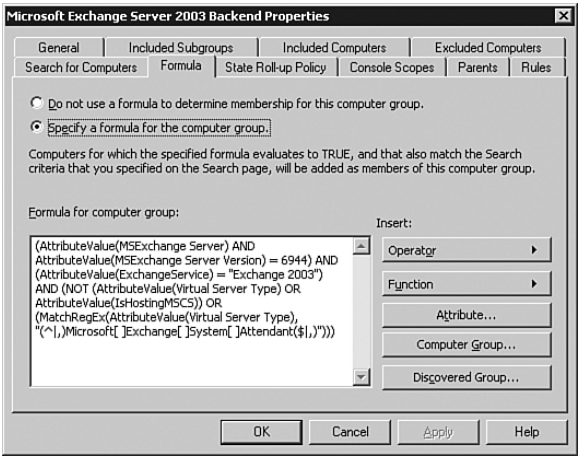


FIGURE 14.37 Microsoft Exchange Server 2003 Backend computer group formula.

As you can see from the formula, the computer group selects members by the MSExchange Server attribute and the MSExchange Server Version attribute that we saw in our previous sample, as well as several others related to Microsoft Cluster Service (MSCS). You can create sophisticated formulas as needed to arrive at the correct memberships. Sophisticated is a euphemism for complex, which is a euphemism for ugly. But sometimes you need that.

Rule Groups

Rule groups allow you to organize and deliver large rule sets effectively. Rules are created in the rule group folders. Rule groups can contain other rule group folders, further organizing the sets of rules. Each rule group contains three predefined folders for the different types of rules, Event Rules, Alert Rules, and Performance Rules. The rules of each type are created in their respective predefined folder.

Continuing with our Exchange 2003 example, you can see the Exchange 2003 rule group in Figure 14.38. (This is one of four rule groups within the Microsoft Exchange Server rule group; the others are Exchange 2000, Exchange Management Configuration Data, and Exchange Service Discovery.) In the left pane, you can see that the rule group has subfolders that address specific areas such as the Availability and State Monitoring, the Exchange Event Monitoring, the Health Monitoring and Performance Thresholds, the Performance Counter Logging, and the Report Collection rule groups. In Figure 14.38, we have selected

the Database Mounted Check rule group within the Availability and State Monitoring rule group. Whew! That is a lot of rule groups and rule subgroups with a lot of rules behind them. The subfolders help organize and manage the rules within the rule groups.

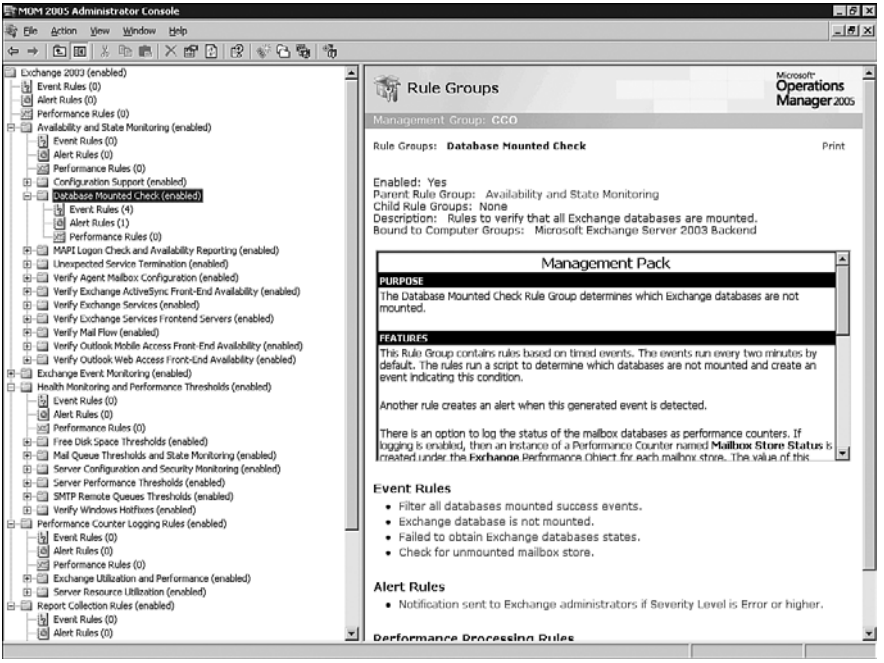


FIGURE 14.38 Microsoft Exchange 2003 Server rule group.

Looking at the right pane toward the top, you can see that the rule group is bound to the Microsoft Exchange Server 2003 Backend computer group. The text explains the function of this specific rule group, provides guidance on configurations, and shows the rules in the group, which in this case check the Exchange databases on managed computers.

The need for the capability to organize and deliver rules effectively is critical when you realize that the Microsoft Exchange 2003 Server rule group alone contains more than 2,000 different rules. Trying to manage that quantity of rules in a flat structure would be a nightmare.

Providers

MOM can monitor information from a number of different sources, called *providers*. However, those providers must be defined prior to being able to monitor them. Microsoft comes with more than 600 predefined providers, and you can add more as needed.

A given provider typically collects one type of data. For example, if you need to collect two different performance counters, you need to create two different providers. There is a variety of different provider types to collect different types of data:

- Windows event log providers—These collect information from the Windows event logs, and the providers for the default logs are predefined, including System, Application, Security, Directory Service, DNS Server, and File Replication Service. You can create additional event log providers if you have additional types of logs by simply typing in their name when creating the provider.
- Windows performance counter providers—These providers collect information from performance counters. You can use a specific target machine to specify the object, counter, and instance to collect, as well as a sampling interval. The sampling interval could be by the number of seconds, minutes, hours, or days. The default is 15 minutes.
- Application log providers—These are application log files, such as the IIS web or FTP server logs. Application log providers also include a generic single-line log file or the Unix Syslog port. The last two allow you to scan any ASCII-text-based log file or to receive Unix Syslog messages, respectively.
- WMI event providers—These collect information from Windows Management Instrumentation, such as service status. For example, you would use this as the source to use to check whether a service is running.
- WMI numeric event providers—This provider type collects information from WMI, such as page faults or processor utilization. This is similar to the information collected by the Windows Performance Counter provider type, but not as easy to select.
- Timed event providers—Timed events provide a way to trigger other events at specific scheduled intervals. They can be scheduled by the number of seconds, minutes, hours, or days. They include a synchronize option that will force the timed interval to start at a specific time.

The most commonly used providers are the performance counter and the event log types. However, the application log type and the WMI type give you an incredible flexibility to instrument almost anything on a Windows platform. The WMI providers use the WQL query language to specify what to collect. See the Microsoft WMI SDK at http://msdn.microsoft.com for more information.

The application log provider can capture information from any text file and take appropriate action based on the contents of the file. Many non-Microsoft applications use text-based log files, which are difficult to parse and find potential problems; MOM can automate this task using the application log provider type. Table 14.4, Table 14.5, and Table 14.6 list some sample providers that come predefined with MOM 2005 and the management packs. Once again, there are close to 700 predefined providers (so no we are not going to list them all here!).

TABLE 14.4 Sample Windows Event Log Providers

Name	Object
Application	Windows Application event log
Security	Windows Security event log
System	Windows System event log
DNS Server	DNS Server event log
File Replication Service	File Replication Service event log

TABLE 14.5 Sample Windows Performance Counter Providers

Name	Object	Counter	Instance	Sampled Every
Processor-% Processor Time-<All>-5.0-minutes	Processor	% Processor Time	<All>	300 Seconds
Web Service-Current Connections-_Total-15-minutes.	Web Service	Current Connections	_Total	900 Seconds
Exchange 2000: MSExchangeIS Mailbox-Client Logons-_ Total-15-minutes (sample)	MSExchangeIS Mailbox	Client Logons	_Total	900 Seconds

TABLE 14.6 Sample WMI Events Providers

Name	Namespace	Query
SNMP Trap Catcher	root\snmp\localhost	SELECT * FROM SnmpNotification
SNMP Extended Trap Catcher	root\snmp\localhost	SELECT * FROM SnmpExtendedNotification

Note that the performance counter providers are specific, all the way down to the instance. The event log providers are more general and monitor all logged events. WMI is much more general and flexible, due to its programmatic nature.

Using MOM Utilities to Monitor MOM

Let's look at some utilities we can use to monitor MOM. Two of these are from the MOM 2005 Resource Kit, and the third is a simple management pack we have developed.

Operator Console Notifier

The Operator Console Notifier is part of the MOM Resource Kit. It provides a simple summary of the status for the servers MOM is monitoring and visual indicators of when server status changes and what that change is (one server changing from green to yellow increases the number of yellow and decreases the number of green). The notification, shown in Figure 14.39, appears in the bottom-right corner of your screen when changes occur and automatically disappears after a short period of time (which is almost enough time to read the notification!). The Operator Console Notifier is an easy way to keep an eye on the high-level status of your monitored servers while working on other tasks.

FIGURE 14.39 Operator Console Notifier status.

The Console Notifier has several options for customization. These items are available by right-clicking on the Operator Console Notifier icon in the system tray:

- Update Counters Now forces a manual update. Updates normally occur on the same interval as your Operator console refresh rate setting (this can be adjusted as part of the Console Settings in the Operator console).
- Show Counters Now forces the notification window to appear, showing current counter numbers.
- Notify on Change when checked (the default) causes the notification window to appear any time a counter changes.
- Auto Hide Notifications if checked (default) causes the notification window to close shortly after appearing.

Response Test Utility

The Response Test Utility (ResponseTest.exe) is a new addition to the MOM 2005 Resource Kit. If you are developing your own response scripts and they fail from a syntax error in the script, MOM displays the error in the Operations console. This is not a particularly efficient way to develop scripts. The Response Test utility provides a quick way to test your response scripts for minor errors from the command line, which can help with developing your own management packs or altering existing scripts.

The utility must be run from the MOM installation directory, which by default is %*ProgramFiles*%\Microsoft Operations Manager 2005. The syntax for ResponseTest is:

```
ResponseTest.exe <options...>
<options>
/config:<path>      The path to the configuration file
/script:<path>      The path to the script file
/out:<path>         The path to the output xml file
/runmode:<runmode>  Either 'emulation' (default) or 'mom'
/f                  Overwrites the output xml file if it exists.
/q                  Suppresses all prompts.
/d                  Enables script debugging.
/x                  Breaks on first line of script.
```

More information on these options are available by running `ResponseTest /?` at the command prompt.

Maintenance Mode Management Pack

Computers monitored by MOM require maintenance just as any other computer systems do. To avoid unnecessary alerts, use the MOM 2005 Operator console to put the computer into maintenance mode during scheduled maintenance periods. Maintenance mode notifies the management server that all new incoming alerts from the computer are automatically set to Resolved.

Computers can be placed in maintenance mode using the MOM 2005 Operator console, by performing the following steps:

1. In the Operator console, choose the Alerts, State, or Computer view in the Navigation pane.

Putting Computers in Maintenance Mode

To put multiple computers into maintenance mode at the same time, use the Computers view rather than the State view. The State view does not allow you to highlight multiple computers and put them into maintenance mode.

2. In the Details pane, right-click the computer and choose Put Computer In Maintenance Mode.
3. On the Maintenance Mode Properties dialog box, you can specify a reason for the maintenance, set the time for the maintenance mode (the default is 30 minutes; a setting of at least 5 minutes is recommended), or set a specific time for maintenance mode to end.

Coding for Maintenance Mode

The MOM Software Development Kit (SDK) can also be used to put computers into and take them out of maintenance mode. The MOM SDK includes three major components: the MOM Connector Framework (MCF), the MOM Management Server Class Library (MCL), and MOM responses to extend MOM rules. The MCL provides capabilities that can alter the maintenance state of a computer. For example, the following code can place a computer in maintenance mode:

```
compMaint.SetMaintenanceMode(comp, EndTime, reason)
```

The MOM SDK is available at http://go.microsoft.com/fwlink/?linkid=50272.

Maintenance mode provides a way to avoid unnecessary alerts caused by scheduled maintenance. To demonstrate an example of the functionality you can build into MOM we created a simple management pack that puts computers into maintenance mode on a scheduled time frame.

The Maintenance Mode Management Pack contains a single rule called Put Computers in Maintenance Mode. It runs by default on Monday nights at 11:20 p.m. (configured under Management Packs \ Rule Groups \ Maintenance Mode \ Put Computers in Maintenance Mode on the Data Provider tab) and runs for computers belonging to the Scheduled Maintenance computer group. The rule runs a response to call the mominfo.exe program to put the server into maintenance for 360 seconds. The steps to install and configure this management pack are as follows:

1. Import the management pack.
2. Create a share called *maintenance* on one of your servers with the mominfo.exe available for execution by servers you will be placing in maintenance mode.
3. Edit the rule, changing the response to refer to the server with the maintenance share on and the amount of time to put the server into maintenance mode.
4. Customize the data provider and schedule screens to reflect your actual maintenance window.
5. Configure the members of the schedule maintenance computer group to reflect the actual servers requiring scheduled maintenance (we suggest trying this on a single server first to test your configuration).

On the CD

The management pack is called the Maintenance Mode Management Pack and is on the CD included with this book.

Maintenance Tuning

Now that we have discussed the different rule components and several utilities to help with monitoring MOM, let's look at some tuning approaches for your MOM environment.

Tuning by Color

An easy way to know the health of your system is to check the state of monitored servers based on their color, as discussed in the "Alerts and State Management" section earlier in this chapter. As you look at opportunities for tuning, red systems should be given the highest priority, yellow the second priority, and green means there is nothing (other than potentially informational messages) to review.

There are multiple approaches you can take: resolving alerts, addressing alerts that need to be scheduled for resolution, changing alert thresholds, disabling rules, customizing rules, and removing dead servers. The actual steps you take will be unique due to the differences in environments, management packs, and standards for each organization.

Resolving Alerts

The preferred approach for resolving alerts is using the product knowledge and the tasks provided with the management packs. Because one of MOM's primary benefits is to assist you with resolving issues in your environment, it is best to work with the information provided for resolving alerts MOM generates. Let's look at several examples:

- Agent will not deploy—Here we address an issue of a MOM agent that will not deploy to a targeted system. For this example, we determined that the agent did not deploy because the Remote Registry Service is not running on the remote system. To resolve this alert, highlight the alert in the Operator console and select the Computer Management task, which initiates the Computer Management MMC console. Using this console, open Services and start the Remote Registry Service. After the service is started you can push install the agent from the MOM 2005 Administrator console.

  After addressing the situation, return to the Operator console and resolve the initial alert. MOM's product knowledge suggests methods that can be used to address each issue, so simply following what MOM tells you to do often resolves the alert.

- Service failure—Let's say that on the Greeley Exchange Server the MSExchangeIS service is not running. To resolve this issue using the MOM Operator console we highlight the alert and click on the Product Knowledge tab, which tells us Exchange monitors a group of services defined by a registry key (HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange MOM) and that for a service failure of this type we should restart the service and investigate why the service stopped. To do this we can again use the Computer Management task—this time from the Services icon to start the Microsoft Exchange Information Store service.

  In the case of a stopped service, we would most likely want to determine why this service was not running. Did someone shut down the service? Or was there some type of service failure on the system? Here you may need to do some additional troubleshooting to determine the cause of failure.

Alerts Follow-up

After you have resolved an alert it is important to see whether it recurs on a regular basis. If the alert continues to appear in the Operator console there is probably an underlying cause that should be addressed before the issue can be completely resolved.

Alerts That Cannot Be Resolved at This Time

You may identify issues in your environment that will require resolution (so you still want to know about them) but that you cannot immediately resolve. This could be due to change control requirements, scheduled downtimes, or even something as simple as time to acquire replacement hardware. Let's look at a situation where our management server, Monarch, is detecting high levels of page fault activity.

We determine that this server does not have enough memory to function effectively as a management server, so for this particular issue we can assign the alert to Level 3 to indicate scheduled maintenance is required. (As mentioned earlier in the "Generating Alerts" section, you can customize these levels in the Administrator console under Administration \ Global Settings \ Alert Resolution States.) We will then order additional memory, and after it arrives submit a change control request to install the memory. We will ultimately resolve this alert within MOM saying that additional memory was purchased and installed into the system.

Already Resolved?

Don't assume that the issue is still valid just because an alert appears. In the Operator console on the Alerts tab, highlight the alert and check the Time of Last Event field. If this time field occurs far enough in the past the issue may already have been resolved, just not closed in the console.

Changing Alert Severity

You may have alerts in your environment that need their severity adjusted due to operational requirements. For example, our Contoso domain has multiple servers to which we manually apply security patches. We want to know which systems cannot connect to the Automatic Updates service, but in our particular environment we do not consider it a critical error if they cannot. We can change the alert severity for this rule from Critical Error (the default) to Informational.

The rule you want to change is located in the Administrator console under Management Packs \ Rule Groups \ Microsoft Windows Servers Base Operating System \ Windows 2003 \ Core System Components and Services \ Event Rules \ Windows is unable to connect to the Automated Update service. Copy and rename this rule and disable the original. Edit the properties of the new rule and on the Alert tab change the Alert severity from Critical Error to Informational. After we Commit Configuration Changes we should no longer see this particular situation causing the server to go to a red or critical state.

Methodology for Modifying Rules

As discussed in Chapter 13 importing management packs will overwrite rules you have changed, even when you use the Update option. Exceptions are information you have added to the company knowledge base, whether you have enabled or disabled a particular rule, and any custom rules added to the management pack. Always copy a rule you are going to change, give it a meaningful name, and disable the original rule. You may even want to put all new rules you create in a separate "custom" management pack, as we have done in this chapter.

Rule Customization

When resolving alerts, consider that additional alerts may be resulting from the alert you resolved. When modifying an individual rule, the type of change varies based on how that rule functions. After examining the rule, you may decide to modify the threshold or

alter its script parameters, or perhaps even change the rule criteria, or the script it executes.

Customizing Rules

Generally, it is best to modify the threshold or alter the script parameters. Altering the rule criteria or the script itself is more complex and should be examined carefully before proceeding.

Changing Script Parameters

You may have rules that are not appropriate for specific servers. For example, we have a database job that runs longer than the 60-minute threshold associated with the SQL Server 2000 Long Running Agent Jobs rule. The Fountain server runs an agent job called SCDWGroomJob; this job runs regularly at 3:00 a.m. and for more than 60 minutes.

One option available is changing the warning threshold in the Administrator console at Management Packs \ Microsoft SQL Server \ SQL Server 2000 \ SQL Server 2000 Health and Availability Monitoring \ SQL Server 2000 Long Running Agent Jobs, by altering the script available on the Responses tab. The warning threshold value is set to 60 minutes by default. Changing the value alters the warning level on all SQL Servers that are members of the Microsoft SQL Server 2000 Agentless Servers or the Microsoft SQL Server 2000 computer groups. Let's go through the steps to do this:

1. Make a copy of the current Management Packs \ Microsoft SQL Server \ SQL Server 2000 \ SQL Server 2000 Health and Availability Monitoring \ Event Rules \ SQL Server 2000 Long Running Agent Jobs rule using the copy/paste functionality in the Administrator console. (The SQL 2005 equivalent of this rule is located in Management Packs \ Microsoft SQL Server \ SQL Server 2005 \ State Monitoring and Service Discovery \ SQL Server Agent Long Running Jobs.)
2. Rename the new rule to be easily differentiated from the rules that come with the management pack. You could append the company name to the beginning of the rule, so in our case the resulting new rule is named Contoso SQL Server 2000 Long Running Agent Jobs.
3. Disable the original rule; change the value for `WarningThresholdInMinutes` in the script parameters to 90 in the copied and renamed rule, and Commit Configuration Changes to complete the process.

The change alters the warning level for all long-running scripts not to provide a warning until a job runs more than 90 minutes. If you do not actually want to do this to all long-running jobs, a better approach would be to create a script parameter override for one or more specific server(s).

Creating New Rule Groups

Another approach to change a threshold specifically for the Fountain server without affecting other SQL Server database servers would be to create a new Computer Group and a new Rule Group, and then add a new rule using the existing Long Running Jobs rule:

1. Create a new Computer Group by right-clicking on Management Packs \ Computer Groups and choose Create Computer Group. We will create a Contoso Fountain group including only the Fountain server.
2. After creating the Computer Group, create a new Rule Group by right-clicking on Management Packs \ Rule Groups and selecting Create Rule Group. Label this rule group Contoso SQL Server 2000 Health and Availability Monitoring to indicate that it is a copy of the original rule group.
3. Copy and paste the original SQL Server 2000 Long Running Agent Jobs rule to this new rule group.
4. Change the thresholds for this rule as discussed in the previous "Changing Script Parameters" section.
5. Set a rule disabling override as discussed in the previous section to disable the original rule for the Fountain server.
6. Add Contoso Fountain as the associated computer group and Commit Configuration Changes.

This change provides one set of thresholds for monitoring long-running jobs on all servers except for Fountain, and a separate set of thresholds that can be set specifically for Fountain.

Rule Disable Overrides

The Systems Management Server (SMS) Management Pack includes a rule that generates an alert when more than 10,000 send requests are queued up to the Site Server over a 3-hour period. If you have a primary site with several secondary sites, or if there are sender bandwidth restrictions in place for the slower links, it may be "normal" to have more than this number of send requests waiting, so you would not want an alert generated for those servers. However, you still need to know about your other SMS servers where 10,000 is an acceptable level for an alert threshold. In this case, you want to create an override for this rule.

The rule is found under Management Packs \ Rule Groups \ Microsoft Systems Management Server (SMS) 2003 \ SMS Servers \ SMS Site Servers – Common \ SMS 2003 Perf Threshold: Site Server Scheduler Send Requests Backlog > 10,000 over 3 hours. To prevent the rule from being replaced the next time you import the SMS management pack, make a copy of the rule, disable the original, and then rename and alter the rule.

Managing Overrides

Overrides are not exported with management packs; be sure to redefine them in your production environment if they were defined in proof of concept or pilot environments. Identify overrides using the Administrator console under Management Packs \ Override Criteria and then manually add them in production.

To create an override, open the copied rule and go to the General tab. Activate overrides by checking the Enable Rule-Disable Overrides for This Rule check box. Change the override name from the default to be more descriptive such as Contoso_SiteServerBacklog_RuleDisable. Set the criteria to add your SMS server to disable (0) for this rule. After making the change, Commit Configuration Changes to complete the process.

You probably still want to be notified of processing backlogs for that Site Server, just at a higher number of requests. One way to do this is make a copy of the rule and change the threshold for the number of send requests. Because this is a state-based rule, you would set the new threshold under the Alert tab, editing the state properties to the new levels. Figure 14.40 shows an example of this.

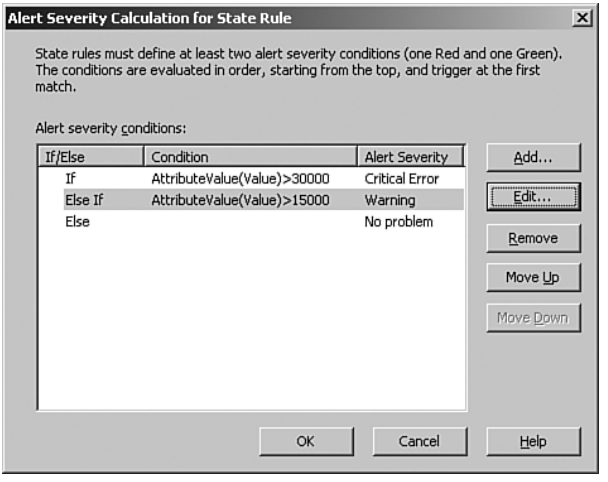


FIGURE 14.40 Setting alert thresholds to determine processing backlogs.

You also need to add at least two entries to the override criteria. First, enable the override for the site server you want to target. Then create a disable override for the SMS Primary Site Servers computer group below the first override. Overrides are read from top to bottom, ensuring that the site server you are targeting receives this rule while the other SMS primary site servers do not. Figure 14.41 shows the override criteria entries.

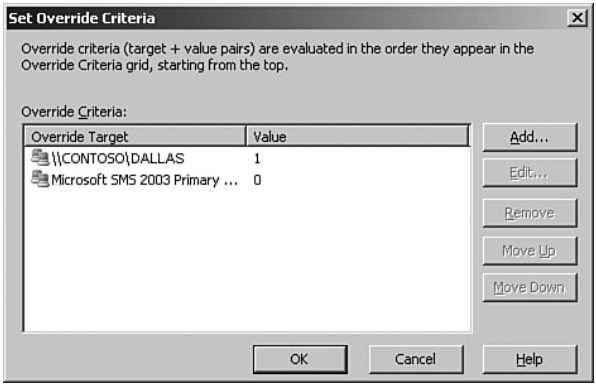


FIGURE 14.41 Adding override criteria.

Criteria Change

Let's look at an example of when you might want to change the criteria applied to a particular rule. Within the Exchange Server Best Practices Analyzer (ExBPA) Management Pack a warning rule is triggered if the SMTP queue folder is located on the same drive as the system partition.

We have a server running on a 1-U rack-mount system with RAID1 drives (mirrored) in a single drive configuration. The server runs Exchange 2003 as an email routing server. We cannot add another drive (due to the disk capacity of the server), so we decide to alter the ExBPA rule by following these steps:

1. In the Administrator console, go to Management Packs \ Rule Groups \ Microsoft Exchange Server Best Practices Analyzer Tool \ Event Rules.
2. Copy the ExBPA Warning rule, disable the original, and rename the new rule to Contoso ExBPA Warning.
3. On the Criteria tab of the new rule click on Advanced, and add a criterion that says when Event Number Not Equals 1371 (the event id of the SMTP queue folder warning). This is shown in Figure 14.42.
4. After completing your changes, Commit Configuration Changes to have them immediately applied.

Alternatives to Changing Rule Criteria

Another approach would be to create a rule override that disables this rule for the specific server to which this warning does not apply; but a side-effect would be to disable all other BPA warnings to this server, so this is not an approach we recommend.

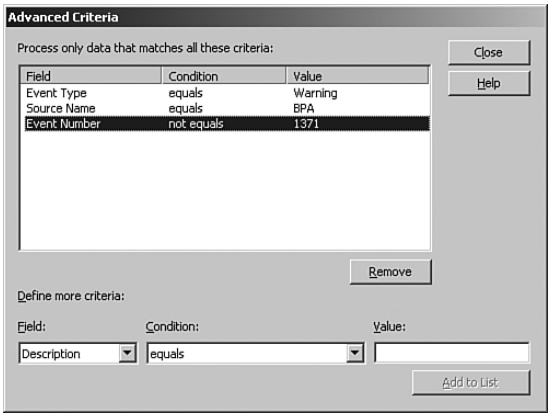


FIGURE 14.42 Adding advanced criteria.

This change removes any warnings within the MOM Operator console from the Exchange Best Practices Analyzer regarding the SMTP Queue folder being on the same drive as the system partition.

Limitations of Changing Rule Criteria

This particular approach only works for a single rule and does not scale up. The solution does not work if you want to stop two or more rules from generating alerts.

Performance Thresholds

Within our Contoso environment, the application database server contains multiple databases providing services to many users, and it is not unusual to have more than 1,000 users connecting to the SQL Server at any point in time. Yet, the SQL Server Management Pack includes a threshold that generates a warning if there are more than 500 SQL Server User Connections.

To change this in our environment we open the MOM Administrator Console \ Rule Groups \ Microsoft SQL Server \ Server Performance Thresholds \ Performance Rules. We copy the SQL Server User Connections > 500 rule and call it Contoso SQL Server User Connections > 1000 rule. We disable the original rule, and go to the properties for our new rule. On the Threshold tab, we can now change the default of 500 to 1000, which is closer to the requirements for this server. After we commit this change all SQL Servers will now generate the warning if they go above 1000 connections instead of the default of 500.

For state-based rules, the threshold value for a performance threshold rule is found within the advanced properties of the Alert tab. The Exchange management pack includes rules that provide an error alert if either of the mailbox store send or receive queues goes above 25. If your server is a routing system providing services many users, this value may not be sufficient. To change the value go to the Administrator Console \ Rule Groups \ Microsoft Exchange Server \ Exchange 2003 \ Health Monitoring and Performance

Thresholds \ Mail Queue Thresholds and State Monitoring \ Performance Rules. Within this folder, there are two Exchange 2003 rules which alert based upon the send and receive queue lengths. The two rules are Mailbox Store: Receive Queue > 25 and Mailbox Store: Send Queue > 25.

To customize one of these rules make a copy, disable the original, and rename the new one in this case to Contoso Mailbox Store: Receive Queue > 100. Set the threshold for the new rule on the properties page by clicking on the Alert tab and clicking Edit on the Alert Properties. Edit the If AttributeValue(Value) > 25 line to the appropriate value; in this case that would be If AttributeValue(Value) > 100. Commit Configuration Changes to apply them immediately. This change alters the error notification threshold for send (or receive) queues for all Exchange servers in the management group.

If we want to change the default threshold but only for specific servers, we can create an override for the performance threshold. For example, we can configure the Aurora Exchange server to have an override stating an acceptable Receive Queue > 100. This changes the threshold for the Aurora server but leaves the remaining servers to the default value of 25.

Scripts

Changing the script itself is an option if you cannot achieve the desired result using the methods discussed previously. Modifying scripts can be complex and should only be undertaken when no other alternative is available. To modify a script, go to the properties of the rule, select the Responses tab, and evaluate the contents of the script. Always retain the original script and work from a copy so that you can restore the original if issues occur with the revised version of the script.

Overtuning

Avoid the urge to *overtune* because sometimes a little knowledge can be dangerous. For example, changing a provider on a counter to sample every 30 seconds versus the default of 15 minutes could increase the information sampled thirtyfold—an example of tuning in the wrong direction!

Let's say that your environment has 200 or so SQL Servers and you change the sampling for three rules. You would get 1.8 million counters rather than the original 60,000, so think about the impact of any changes you may make.

Also, providers are highly shared throughout MOM. Changing a provider when customizing one rule changes it for all rules using that provider!

Searching for Rules

More than 6,000 rules are in the default installation of MOM 2005 when you include shipping management packs. These are organized into close to 300 rule groups. Trying to find a specific rule within all the processing groups by browsing though them is akin to finding a needle in a haystack. In other words, it is extremely difficult to do.

Fortunately, the Administrator console gives you a flexible and powerful search tool to locate the rules based on a wide variety of parameters.

Rule Search Options

The search engine has a number of different options to allow effective searches. The search specification can include the following:

- Location—The location can be all rule groups, or you can select a specific rule group to search. Rule groups that exist under the one you specify are automatically searched.
- General—You can search by rule name, wild card match, rule type, and/or modification. You can specify all rule types or choose one of the rule types. If you choose a specific rule type, it changes the search windows to allow you to enter more specifics under provider and criteria as appropriate.

  You can also specify modification by date and/or by user. This is useful if you are trying to track down rules modified during a certain time frame or by a particular user.
- Override types—You can search by override types, including rule disable, performance threshold, script parameter, and state alert severity. You can also search by override name and by the criteria type (set, not set or both).
- Provider—If you select the event or rule type search, the provider window becomes available. The provider window lets you specify a provider wild card match and/or provider types.
- Criteria—If you select the event, alert, or rule type search, the criteria window becomes available. The window is different for each of the rule types, allowing you to match the criteria specifications germane to each rule type.
- Responses—Responses allows you to search based on a specific script launched in a rule or a particular notification group. The other responses are not searched, unfortunately.

This wealth of search options makes it easy to track down the precise rule you are looking for. We will now run a rule search to get a feel for it.

Finding Rules

Let's run an example search. For example, suppose that we need to find any rule that uses the Web Service Current Connection provider from the table (Web Service-Current Connections-_Total-15-minutes).

To run the search, follow these steps:

1. In the Administrator console, select the Rule Groups node.
2. Click on the Action menu and select Find Rules.

3. Click Next to search in all rule groups.
4. Select the Performance rule type and click Next.
5. Click Next to skip past the override section.
6. Check the Provider Name box.
7. Set the provider name match to contain a substring.
8. Enter **Web Service-Current Connections** in the provider name and click Next.
9. Click Next to leave the criteria blank.
10. Click Finish to leave the responses blank and execute the search.

Figure 14.43 shows the results we get. As you can see, it found two measuring rules where this particular provider is used.

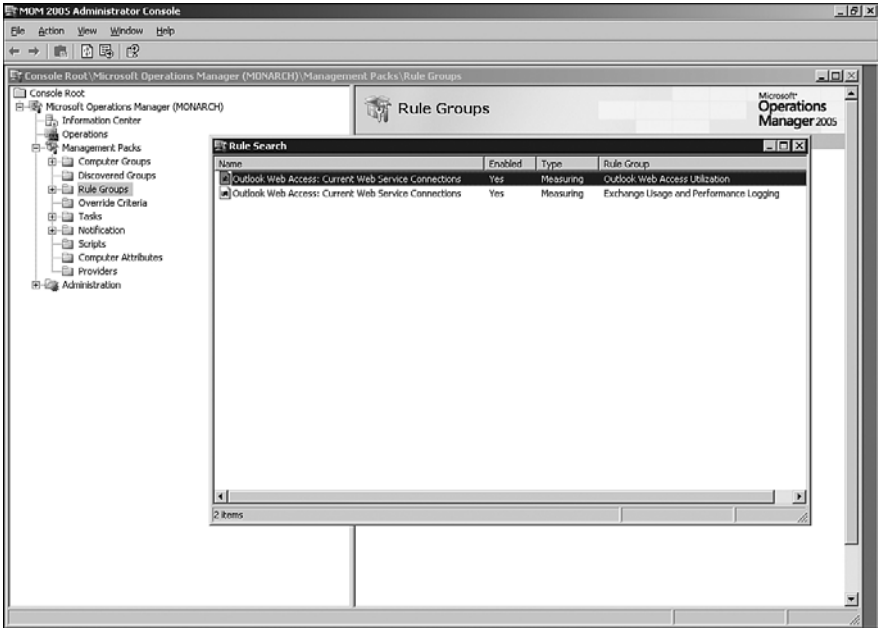


FIGURE 14.43 Rule search results.

This capability allows you to track down rules quickly in a variety of ways. Given the huge number of rules in MOM 2005, this is a useful feature.

Viewing the Results

For every search you make and don't close the window, you can go back to view it. You can also update the view by refreshing, and it will regenerate the view.

To view a previously generated search, perform the following steps:

1. In the Administrator console, expand the Management Packs node.
2. Expand the Rule Groups node.
3. Expand the Search Results node.
4. Select the Rule Search node to view the previous results.

If the rules have changed since you ran the search, you can press F5 to refresh the view, and it will update based on search options you specified. If you generate a view based on the date and time, it might not reflect changes because it will only find events that occurred within the window of time. Although you specify the date in the search options for date, the interface actually fills in a date and time. The time is the current time, so it misses any updates after the current time.

Rule Statistics

The rule types are not evenly distributed through the management packs Microsoft provides. The common management packs include more than 6,000 rules, but Table 14.7 shows that the event rule class is by far the most utilized rule class with about 88% of the rules that ship in the management packs. The performance class of rules is a distant second at about 10% of total number of rules. To really bring the disparity home, the information is also displayed graphically in Figure 14.44.

TABLE 14.7 Management Pack Rule Distribution

Rule Class	Rule Type	Number in Management Packs	% of Total
Event	Event	5,178	83.09%
	Consolidation	179	2.87%
	Collection	73	1.17%
	Pre-Filter	16	0.26%
	Missing	1	0.02%
Performance	Measuring	523	8.39%
	Thresholds	115	1.85%
Alert	Alert Processing	147	2.36%
Totals		6,232	100.00%

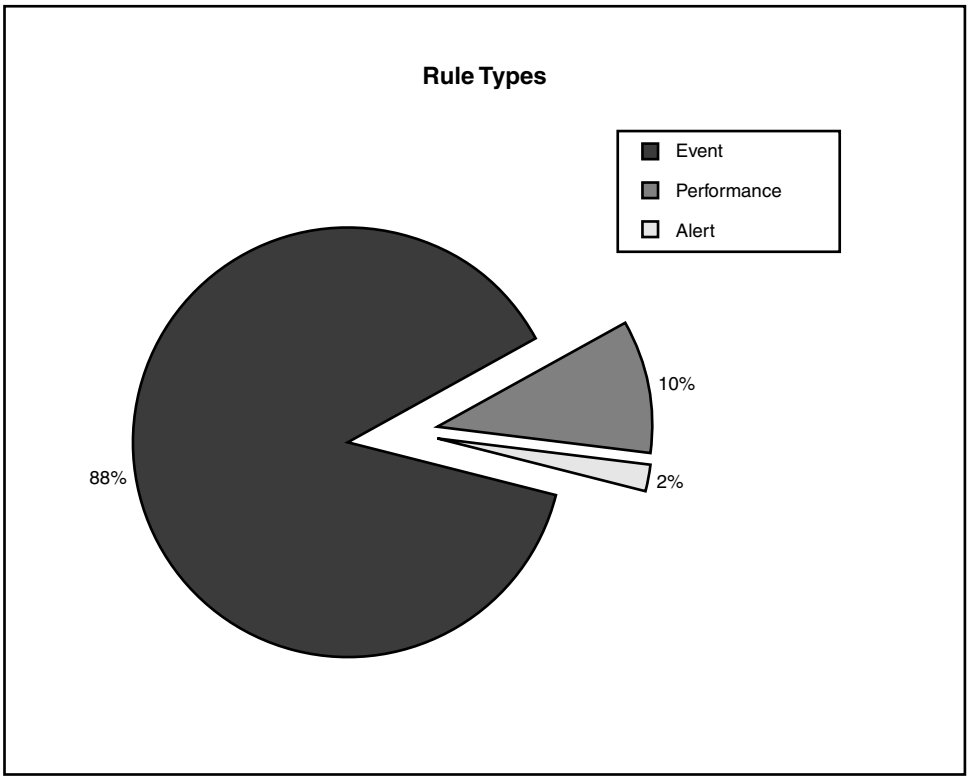


FIGURE 14.44 Overall rule type distribution.

If you have a sharp eye for numbers, you might notice that the total count of rules in Table 14.7 exceeds the count of the management pack rules on the Detail pane of the Management Pack node in the MOM Administrator console. This is because the Detail pane reports on enabled rules only and ignores the disabled ones. The previous statistics reflect the total number of rules, even if they are not enabled.

The number reflected in your environment will vary depending on the management packs installed, but the overall proportions are representative.

Within the event rule class, you can also see there is a disparity in the rule types as well. The event rule type within the event class has more than 95% of the total count of event rules (shown in Figure 14.45). The event rule type is clearly the workhorse of the MOM 2005 business logic. These rules do the majority of problem detection, alerting, and active monitoring for the managed computers. These are the rules that launch scripts and generate synthetic transactions as well.

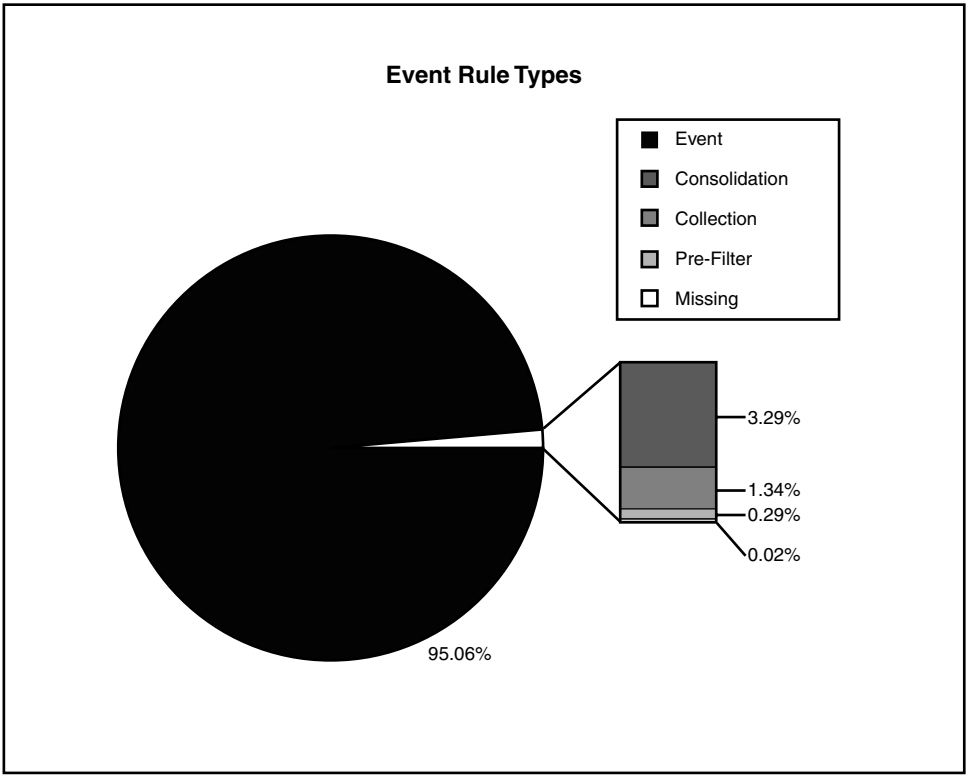


FIGURE 14.45 Event class rule distribution.

Summary

This chapter discussed the different types of rules available in MOM, which include event rules, performance rules, and alert rules. We investigated the major different subtypes of each rule type and discussed alerts and how they work as the tracking mechanism within MOM. We also discussed examples of how to tune your MOM configuration using the information presented about different rule types in this chapter. Next, we discussed how rules are targeted and the role of providers within MOM. We finished the chapter with a discussion on how to find rules and a breakdown of the statistical usage of the different types of rules within MOM management packs. The next chapter discusses how to manage the operating system using MOM.

PART V

Managing with MOM

IN THIS PART

This page intentionally left blank

CHAPTER 15

Managing the Operating System

IN THIS CHAPTER

When a core business application performs badly or becomes nonfunctional, the operational requirement is to "fix it now." Most effort spent monitoring production environments focuses on the functionality and availability of business-critical services and applications. Certainly, it is important to keep core applications functioning, but it is also important to keep an eye on the underlying causes of dysfunctional applications because malfunctioning applications are sometimes only symptoms of more fundamental problems.

Fundamental problems can occur at many points in the computing environment. The environment contains mundane elements that can go awry, such as electrical power, but also elements that may be of more interest to readers of this book: networking devices, computing equipment, and—the focus of this chapter—operating systems running within the network. This chapter focuses on monitoring and managing the operating systems that our core business applications rely on.

The Underlying Operating System

In some Information Technology (IT) environments, the approach taken by administrators is to install the operating system, antivirus software and other components and applications and then, apart from patching the system, leave things alone until there is a crisis. A better strategy, obviously, would be to proactively monitor our production servers. There are four major areas of concern when monitoring server operating systems:

- Stability—Is the operating system functional and responding to network requests? This is the most critical area for server monitoring. If a server is not stable, its performance and functionality are irrelevant.
- Performance—After you have determined that the server is indeed running, how is it performing? Are bottlenecks causing the server to achieve less than optimal performance? How has server performance changed during the last three or last six months? These are the types of questions we want answers to so that we can provide a solid foundation for our business services and applications.
- Functionality—Servers are installed to provide some form of functionality for the business. This could be a Human Resources (HR) application or capabilities such as file and print services, or terminal server access for users. The ability to monitor server functionality is critical to providing a solid monitoring solution.
- Security—A server needs to be secured to provide information only to authorized users. Servers also need to be patched to address critical vulnerabilities. If the server is not effectively secured and patched, it is not a question of whether it will be hacked but when (particularly if the server is Internet facing).

MOM 2005 works to provide the information you need to monitor your Windows operating systems in these four areas, helping you proactively address issues before they impact the functionality your servers are providing. As discussed in other chapters, MOM provides monitoring functionality through management packs. When monitoring the Windows Server operating system, the primary management pack to use is the Windows Server Base Operating System Management Pack.

Windows Server Base Operating System Management Pack

The Windows Server Base Operating System Management Pack (MP) goes a long way toward meeting the highlighted areas of concern for monitoring your Windows operating systems. The management pack monitors the performance and stability aspects of the operating system (OS), and performance tracking allows you to identify potential bottlenecks in the OS while determining trends in utilization on your servers.

Performance

Using the Server Base OS MP, MOM 2005 provides real-time performance and historical performance analysis for Windows operating systems. Four common components are monitored: Processor, Disk, Memory, and Network. We will investigate how MOM manages the operating system through monitoring these four components.

Processor

Processor utilization is the primary metric for monitoring system performance. As a general rule, prolonged utilization greater than 80% may indicate a processor bottleneck

(this is a common benchmark when attempting to identify a bottleneck and not a MOM-specific concept). The Server Base Operating System Management Pack tracks processor utilization and provides notification if a processor exceeds a specified criterion. The rule monitoring processor utilization is located under Management Packs \ Rule Groups \ Microsoft Windows Servers Base Operating System \ <*Windows version*> \ State Monitoring and Service Discovery \ Performance Rules \ Performance Threshold: Processor\% Processor Time threshold exceeded. This rule alerts you if processor utilization is greater than 95% over a sampled period of 5 minutes (which is configurable for your environment).

Another condition that often indicates a bottleneck is a high processor queue length. When this metric is greater than two for a period of time it indicates that the processor cannot keep up with its processing requests. MOM monitors this condition using the same rule that monitors % Processor Time (discussed in the preceding paragraph). This rule's criteria also provides notification when the processor queue for any processor is greater than 15 over a sample time of 5 minutes. These levels are configured from the Responses tab, using the script parameters of `CpuPercentageThreshold` and `CpuQueueLenThreshold`. What we have here is combining monitoring of processor utilization and processor queue length to more accurately determine whether a processor bottleneck exists!

Additional rules check conditions such as whether the percent of time the processor spends receiving or servicing deferred procedure calls is more than 15%, which also indicates potential processor bottlenecks.

The management pack also gathers metrics specifically for use in providing trends in processor utilization. These rules are located under Management Packs \ Rule Groups \ Microsoft Windows Servers Base Operating System \ <*Windows version*> \ Performance \ Performance Rules. The rules collecting processor information include

- Performance Measuring: Processor\% Interrupt Time_Total
- Performance Measuring: Processor\% Processor Time_Total
- Performance Measuring: System\Context Switches/Sec
- Performance Measuring: System\Processor Queue Length

These rules are examples of how MOM 2005 gathers information to provide utilization trending information for systems, which can then be accessed using MOM Reporting. For example, if average processor utilization on a system was 80% at the beginning of the year and has steadily increased to 90% by the end of the year, it is reasonable to project that processor utilization may become a bottleneck the following year. You can also use these statistics to assess multiple systems and their processor utilization over a period of time, as illustrated in the report displayed in Figure 15.1.

MOM Reporting also gives us the ability to show the processor queue length over a period of time, in this case for a single server as shown in Figure 15.2.

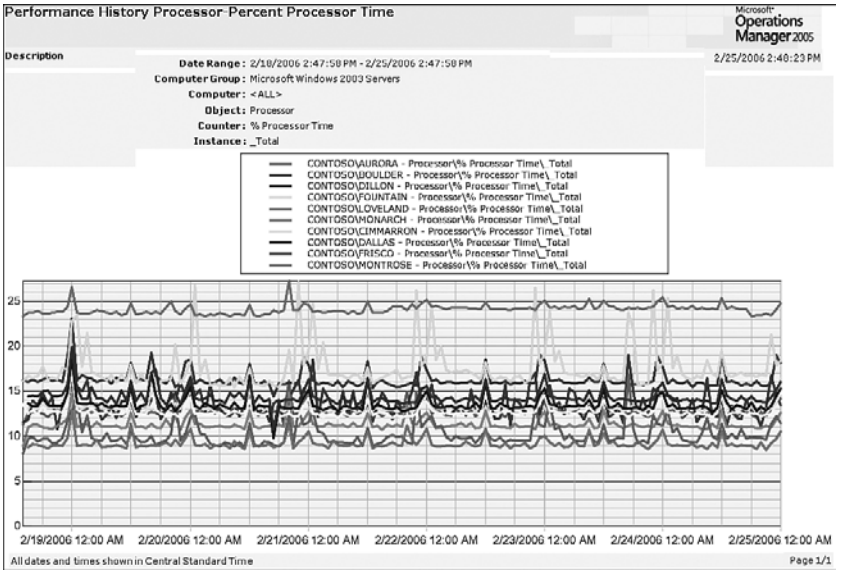


FIGURE 15.1 Percent Processor Time report.

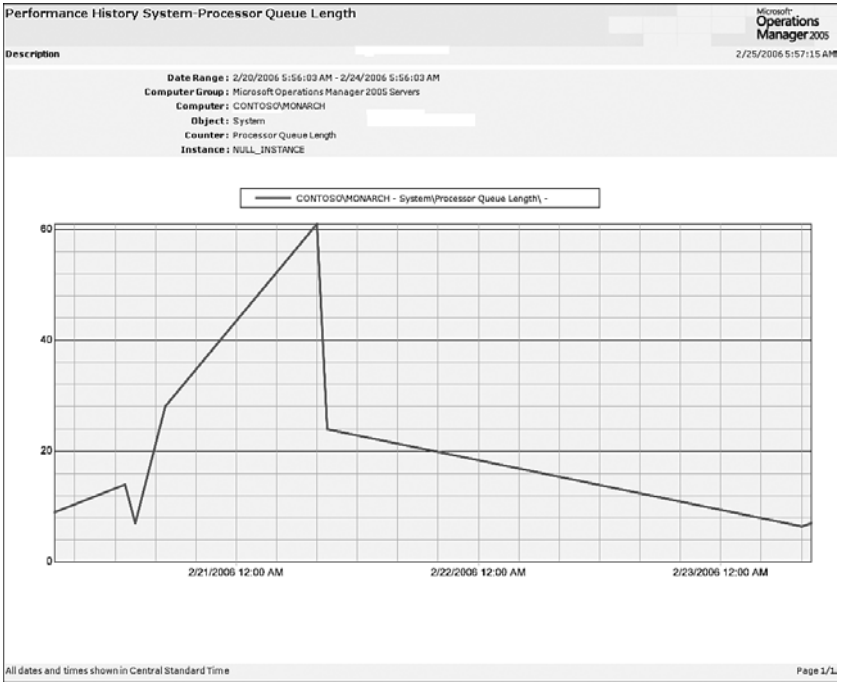


FIGURE 15.2 Processor queue length.

You can customize performance history reports to view metrics not shown in the built-in reports included with the Server Base Operating System MP. Metrics such as % Interrupt Time can be shown using the Performance History report, located within the Reporting console under Microsoft Operations Manager Reporting \ Microsoft Windows Base Operating System \ Performance History. Running the report allows you to specify the name of an object and counter so that you can report on any metrics MOM gathers.

The rules that track processor utilization can also be changed to reflect the requirements of your particular environment. For example, let's look at the rule providing alerts for high processor utilization, which is shown in Figure 15.3. This rule is the same one we discussed earlier at the beginning of the "Processor" section of this chapter and is located under Management Packs \ Rule Groups \ Microsoft Windows Servers Base Operating System \ <*Windows version*> \ State Monitoring and Service Discovery \ Performance Rules \ Performance Threshold: Processor\% Processor Time threshold exceeded.

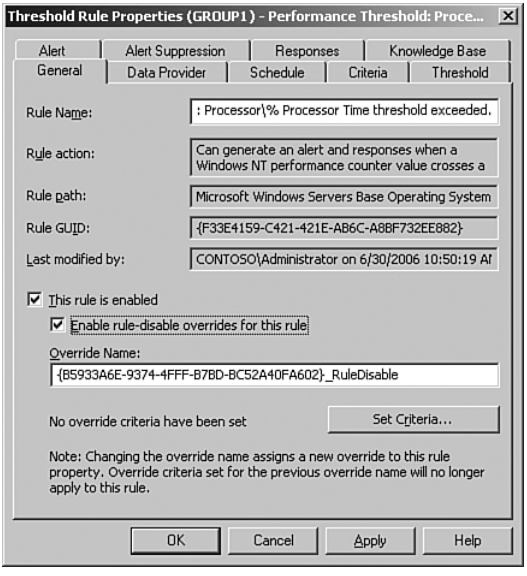


FIGURE 15.3 Processor time threshold rule.

You can tune the rule's thresholds rule by changing the parameters on the Responses tab. If you have specific servers where high processor utilization is not a concern, you can exclude them from being monitored by creating an override that excludes a server from that particular criteria. Figure 15.4 shows the rule disabled for a server named Loveland.

With the Base Operating System MP, MOM can inform you of high processor utilization and gather important metrics to help you determine processor utilization trends on your servers. The management pack also provides this functionality for disk-related utilization.

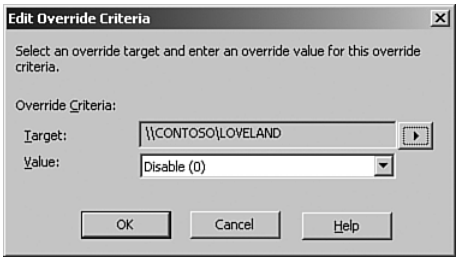


FIGURE 15.4 Configuring override criteria.

Disk

Disk performance is another important aspect of managing performance of your Windows operating systems. As with processor utilization, MOM tracks system disk utilization, both to alert for high utilization and to provide trending information. The management pack also tracks counters such as the amount of available disk space, but we will discuss those counters in the "Stability" section later in this chapter.

MOM gathers counters for average disk read and write metrics. If the average disk reads or writes are greater than 50 when sampled (every 5 minutes by default), a warning alert is generated. There are two alert rules, located under Management Packs \ Rule Groups \ Microsoft Windows Servers Base Operating System \ <*Windows version*> \ State Monitoring and Service Discovery \ Performance Rules:

- Performance Threshold: PhysicalDisk\Avg. Disk sec/Write threshold exceeded
- Performance Threshold: PhysicalDisk\Avg. Disk sec/Read threshold exceeded

Like the processor utilization rule, these two rules can be tuned for your particular requirements or overridden if specific servers should be excluded from disk utilization monitoring.

Disk Monitoring and the Exchange Management Pack

Monitoring performance metrics also takes place in management packs available for specific applications. For example, the Exchange management pack has a rule (under Rule Groups \ Microsoft Exchange Server \ <*Exchange version*> \ Health Monitoring and Performance Thresholds \ Server Performance Thresholds \ Disk Read Latencies > 20 msec). This rule provides notification if performance is not within the ranges expected in this case by Exchange servers. The alert is shown in the Operator console in Figure 15.5.

You may be asking why this rule is in the Exchange management pack rather than the Base Operating System management pack. Management packs are created by the product groups that write each product. Each group may identify performance thresholds that represent a potential warning or error condition for that particular application.

Although it may be acceptable for the operating system to have latency of more than 20 msec, it does represent an issue to the performance of a system running Microsoft Exchange if the latency is greater than 20 msec.

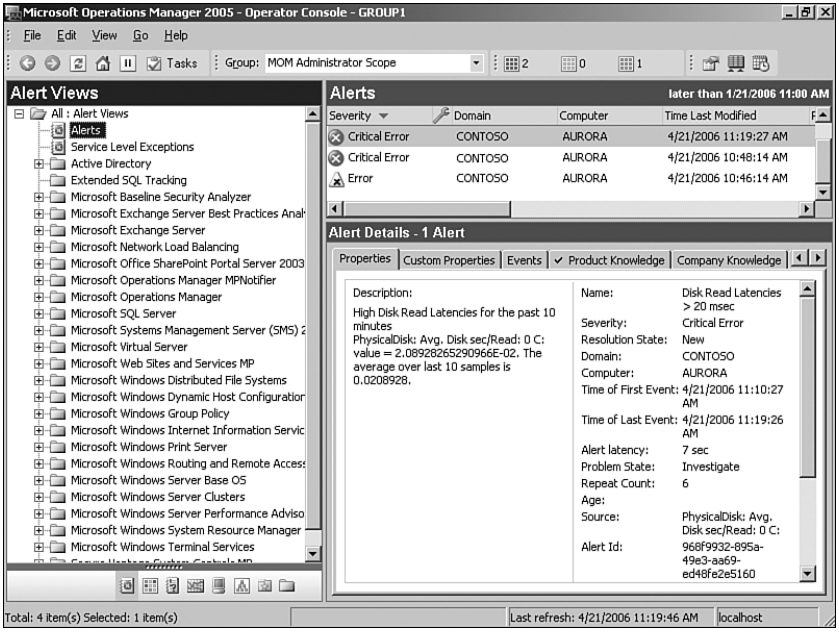


FIGURE 15.5 Exchange management pack disk performance alerts.

The Windows Server Base Operating System MP provides a prebuilt report to track disk performance for trending purposes. This report is the Avg Disk Queue Length report shown in Figure 15.6.

Additional counters that relate to disk utilization can be viewed with the Reporting console in the Microsoft Windows Base Operating System \ Performance History \ Performance History report.

Memory

Monitoring system memory is also a major consideration when monitoring system performance. MOM uses multiple rules to monitor memory utilization. Once again, these rules are located under Management Packs \ Rule Groups \ Microsoft Windows Servers Base Operating System \ <*Windows version*> \ State Monitoring and Service Discovery \ Performance Rules. There are three rules related to memory that generate alerts:

- Performance Threshold: Memory\% Committed bytes In Use threshold exceeded
- Performance Threshold: Memory\Available MBytes threshold exceeded
- Performance Threshold: Memory\Pages/Sec threshold exceeded

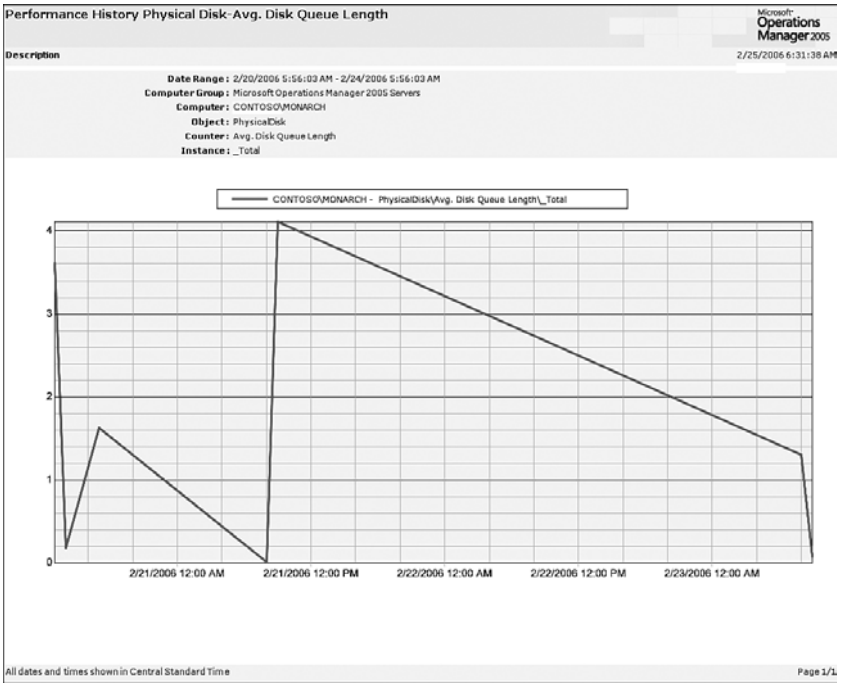


FIGURE 15.6 Average Disk Queue Length report.

The committed bytes rule generates a critical error if the percent committed bytes exceed 80%. The available MBytes rule generates an alert when the amount of physical memory is less than 2.5 megabytes (MB). The third rule is initially disabled, but when enabled it creates a critical error alert if there are more than 50 pages/second. This rule is disabled by default because it is important to first establish a baseline to gauge what an excessive paging value should be for the majority of your systems.

As with the processor and disk metrics, specific memory statistics are gathered to provide trending information. A variety of reports are available related to tracking system memory. These reports include Available MBytes, Page Reads per Sec, Page Writes per Sec, Paging File Percent Usage, Pool Nonpaged Bytes, Pool Paged Bytes, and Pages per Sec (illustrated in Figure 15.7).

The processor, disk, and memory counters are available in a single report, shown in Figure 15.8. This report provides a quick assessment of the most critical metrics when trending system utilization.

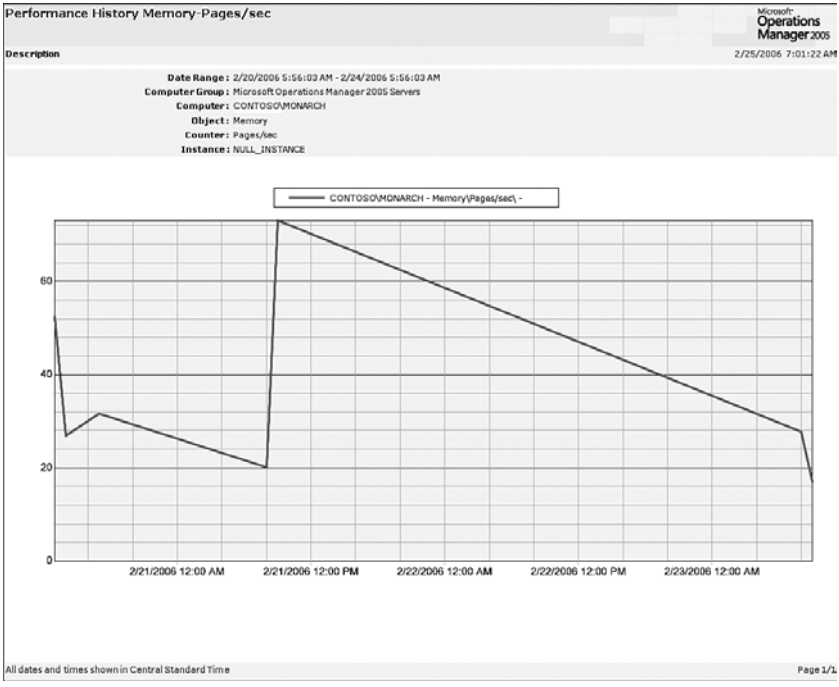


FIGURE 15.7 Pages per Second report.

Operating System Performance

Microsoft Operations Manager 2005

Description 2/25/2006 2:27:10 PM

Date Range: 2/18/2006 2:26:17 PM - 2/25/2006 2:26:17 PM
Computer Group: Microsoft Windows 2003 Servers

	Processor		Memory		Disk		
Server Name	**% Utilization**	**Queue Length**	**Available (MB)**	**Pages/Sec**	**% Free Space (Total)**	**Avg. Disk sec/Read (Total)**	**Avg. Disk sec/Write (Total)**
CONTOSO\AURORA	12.87	8.01	102	15.06	89.33	0.0117	0.0060
CONTOSO\BOULDER	13.64	2.66	149	7.48	68.84	0.0141	0.0033
CONTOSO\CIMMARRON	13.34	1.11	82	0.10	87.64	0.0008	0.0047
CONTOSO\DALLAS	13.52	2.17	23	1.41	72.54	0.0103	0.0065
CONTOSO\DILLON	16.33	7.42	63	14.79	90.20	0.0122	0.0112
CONTOSO\FOUNTAIN	17.62	4.11	56	6.70	32.13	0.0156	0.0031
CONTOSO\FRISCO	14.39	2.91	38	7.32	54.08	0.0104	0.0091
CONTOSO\LOVELAND	11.35	2.69	37	9.97	74.61	0.0140	0.0058
CONTOSO\MONARCH	10.21	3.04	95	1.70	85.09	0.0089	0.0022
CONTOSO\MONTROSE	9.23	1.29	26	0.75	82.09	0.0118	0.0036

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

FIGURE 15.8 Operating System Performance report.

Network

Unlike processor, disk, and memory statistics, network information gathered alerts for high network utilization are not generated. The Base Operating System MP does, however, track information that is available in MOM Reporting as trending information.

Additional counters that relate to network utilization can also be accessed in the Reporting console in the Microsoft Windows Base Operating System \ Performance History \ Performance History report, which we introduced in the "Disk" section of this discussion. The report allows you to choose specific counters to view including those that gather disk utilization statistics. For this particular example, Figure 15.9 shows the total network bytes per second.

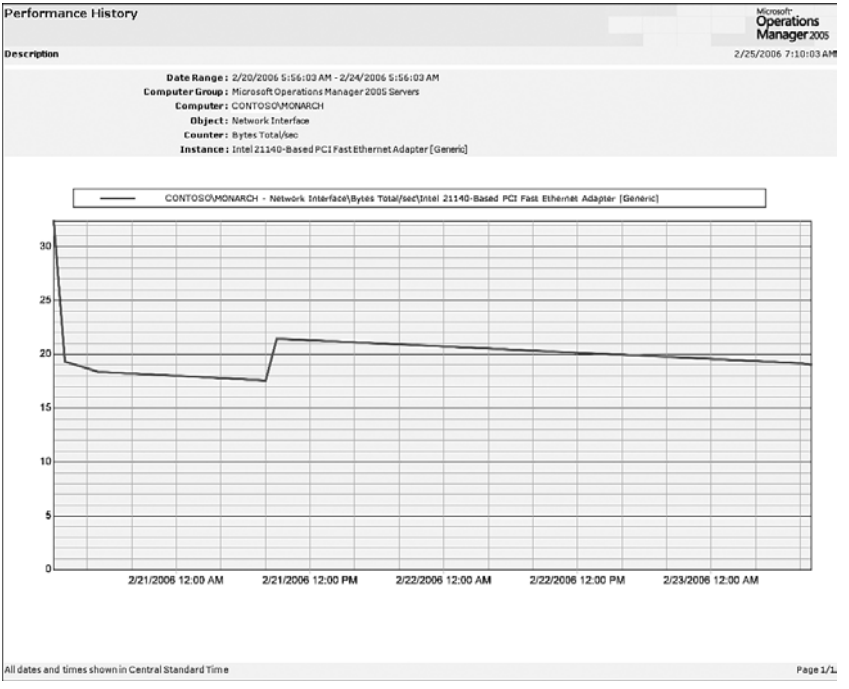


FIGURE 15.9 Performance Report showing Network Bytes Total per Second.

The ability to track performance and provide trending information is important when monitoring operating systems. However, if the system is not stable, its performance is somewhat irrelevant. Let's look at what the Base Operating System Management Pack provides for monitoring operating system stability.

Stability

The Windows Server Base Operating System Management Pack assists in providing a stable operating system by monitoring operating system components and the Windows operating system itself.

System Components

The various system components discussed in the "Performance" section earlier in this chapter (processor, disk, memory, network) also have rules that check for stability. For example, various network-related issues can be identified and will generate alerts. The rules monitoring network stability are located under Management Packs \ Rule Groups \ Microsoft Windows Servers Base Operating System \ <*Windows version*> \ Networking \ Event Rules. These rules include checks for a disconnected network adapter, duplicate names on the network, or Internet Protocol (IP) address conflicts.

There are also rules to monitor the reliability of disk components. These rules are found under Management Packs \ Rule Groups \ Microsoft Windows Servers Base Operating System \ <*Windows version*> \ Storage \ Event Rules. These rules check for chkdsk errors, logical disk manager failures, and NT File System (NTFS) errors, including file system corruption and lost disk writes. Disks are also monitored for available free space. Figure 15.10 shows the default values provided for the Windows Storage State Monitoring script used by the Run Storage State Monitoring rule, located under Management Packs \ Rule Groups \ Microsoft Windows Servers Base Operating System \ <*Windows version*> \ State Monitoring and Service Discovery \ Event Rules \ Run Storage State Monitoring.

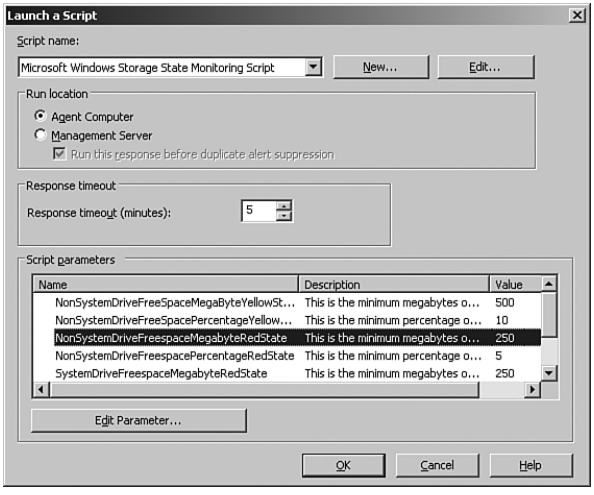


FIGURE 15.10 Storage State Monitoring script default parameters.

As you can see in Figure 15.10, there are multiple parameters including the one highlighted, which is the `NonSystemDriveFreespaceMegabyteRedState` parameter. This parameter sets the level that MOM categorizes as critical should free space on a nonsystem drive drop lower than the specified value, which by default is 250MB. We can change this value if we want to alter it for our specific configuration. Between the parameters listed in this rule and the ability to create overrides, the rule can check most disk conditions. For example, to change the `NonSystemDriveFreespaceMegabyteRedState` critical value you would click on it and change it as shown in Figure 15.11 (where we decrease the value

from 250MB to 50MB), with the result that MOM will not generate a critical level for drive space on nonsystem drives until less than 50MB of disk space is available.

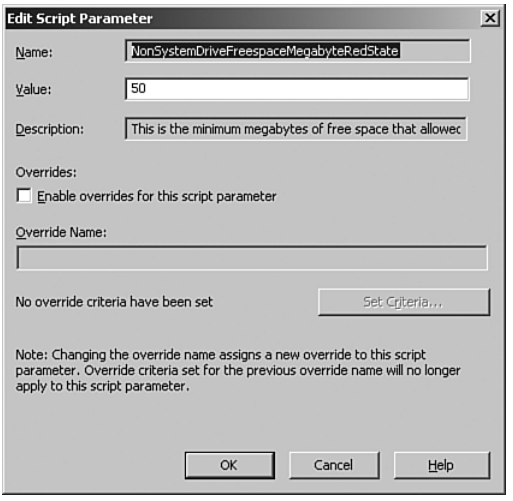


FIGURE 15.11 Changing the `MegaBytesFreeSpaceThreshold` parameter.

There are a number of conditions where this rule does not work well—for example, in an environment where systems typically have drives low on free space. By customizing the Storage State Monitoring rule and creating overrides, the best solution without changing a script would be to create an override for the system with the drive with limited space.

Changing Scripts

Generally you should not change scripts within MOM—Microsoft does not support script changes, and your changes may be lost during management pack updates. But there are times when the only way to provide the functionality you need is by customizing a script.

As provided by Microsoft, the Storage State Monitoring script works by alerting when disk space is less than the specified percentage amount of free space AND less than the specified number of megabytes of free space. As an example, let's take a nonsystem drive that is being monitored with the default parameters to 250MB and 5% free space to alert as critical. This drive is 100 gigabytes (GB) in size and has 4GB in free space.

The drive matches the criteria to create a critical alert based on the percentage of free space (4%) but does not match the criteria to create a critical alert based on the amount of free space (4GB is much larger than 250MB, of course). Given its current condition the drive would not generate an alert. Using this example, this drive would not list as critical until there was less than 250MB of free space, which is actually only .25% (a quarter of a percent) free space.

To monitor disk space when different servers have varying amounts of acceptable free space, you can create overrides that set the limits for all drives to the smallest amount of free space on the system. For example, if server Loveland has a D: drive with only 5% free space, you could override the existing script parameters on the rule to configure a different threshold for the Loveland server. The problem with this change is that now all nonsystem drives on Loveland are set to a threshold of 5% free disk space. If you have a nonsystem drive that you want to be notified when it reaches 10% free disk space and another on the same system where you want to be notified when it has 5% free disk space, using overrides on the Storage State Monitoring script will not meet your business requirements.

Often systems have disk drives that should be excluded from free space monitoring or need individual free space thresholds configured for different drives. For example, there are applications that create nondynamic page files on multiple drives that are configured to use a large portion of the drive, often leaving only a few megabytes of remaining free space. For most organizations it is enough to exclude these drives from free space monitoring. Situations such as these are why the Windows Storage State Monitoring script is one of the most frequently modified MOM scripts. The need for additional granularity in monitoring free space has led many MOM administrators to change the script the rule uses to check free disk space. Appendix E, "Reference URLs," provides links to websites where other administrators share changes made to this script, which will exclude drives from being monitored or set individual thresholds on drives.

We provide a modified version of the Windows Storage State Monitoring Script that allows you to exclude a drive by creating a drive_exclude.mom file on the drive that you want to exclude. The script included on the CD has been altered to make it easy to locate and remove the change if required. The script has comments indicating the beginning and the end of the change. Removing the change only requires removal of the code between the start and end comments (both labeled with `Custom Script Change`). To implement the script, make a copy of the rule and disable the original; on the new version of the rule open the Response tab, edit the properties for the script, and cut and paste in the contents of the script.

On the CD

The modified Windows Storage State Monitoring Script is included on the CD with this book.

Operating System

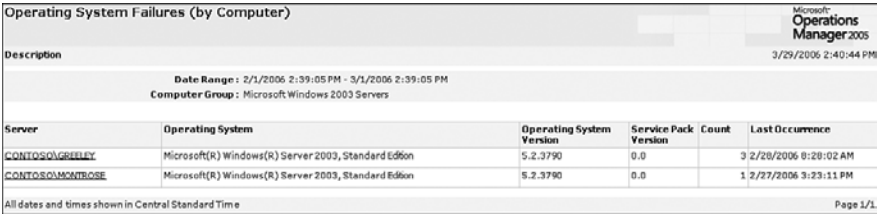
Although it is important that your operating system perform without bottlenecks, it is also essential that a server be stable and can be relied on to perform its function. The Windows Base Operating System Management Pack helps to identify issues that may negatively impact the reliability of the servers you are monitoring.

The rules monitoring operating system reliability are available under Management Packs \ Rule Groups \ Microsoft Windows Servers Base Operating System \ <*Windows version*> \

Reliability \ Event Rules. The management pack monitors applications that generate errors that may impact the operating system. It also monitors system restarts or shutdowns that impact system availability.

One of the rules in the management pack checks for applications generating more than four Dr. Watson errors in a period of 15 minutes (Dr. Watson is a Windows utility that gives details about application crashes in Windows). Other rules check for reboots that have occurred from bug checks. The MP also monitors the status of systems that have experienced a shutdown (dirty, clean, now online, or offline). These rules notify you of errors that impact your server and assist in determining root causes and then resolving them.

Analogous to the performance metrics this management pack gathers, metrics on stability are also collected and can be viewed using MOM Reporting. Figure 15.12 shows an example report with the number of Operating System Failures for a group of computers.



Operating System Failures (by Computer)

Microsoft Operations Manager 2005

Description

3/29/2006 2:40:44 PM

Date Range: 2/1/2006 2:39:05 PM - 3/1/2006 2:39:05 PM
Computer Group: Microsoft Windows 2003 Servers

Server	Operating System	Operating System Version	Service Pack Version	Count	Last Occurrence
CONTOSO\GREELEY	Microsoft(R) Windows(R) Server 2003, Standard Edition	5.2.3790	0.0	3	2/28/2006 8:28:02 AM
CONTOSO\MONTROSE	Microsoft(R) Windows(R) Server 2003, Standard Edition	5.2.3790	0.0	1	2/27/2006 3:23:11 PM

All dates and times shown in Central Standard Time

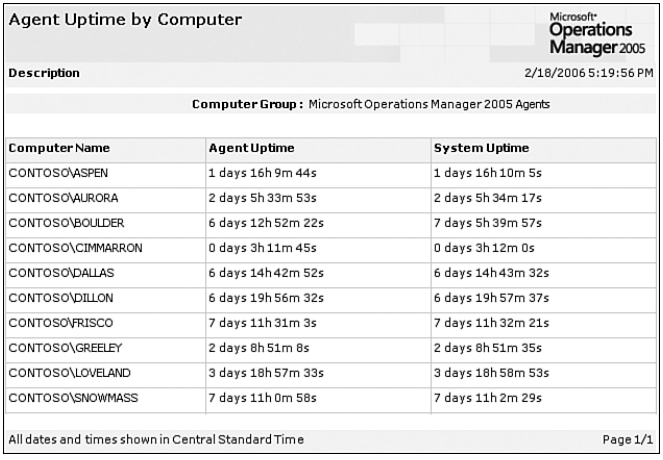
Page 1/1

FIGURE 15.12 Operating System Failures by Computer report.

The Operating System Failures by Computer report is one of the many reports within the management pack that provide information on application and operating system failures. Each report is customized to provide information by application, computer, or event.

Using the MOM Management Pack to Monitor the Operating System

As you read through how the Windows Server Base OS MP works to provide performance information and assist with increasing operating system stability, it may appear that there is a gap in what is required to properly monitor the operating system. This management pack does not notify you if the server is actually running or responding to network requests. That particular functionality is available with the MOM 2005 Management Pack. System uptime/downtime is tracked by monitoring an agent's heartbeat. Figure 15.13 shows an example of information gathered by the MOM MP (this report can be found in the Reporting console under Microsoft Operations Manager Reporting \ Microsoft Operations Manager \ Agent Uptime by Computer). Additional details on the heartbeat are discussed in Appendix A, "MOM Internals."



Agent Uptime by Computer

Microsoft Operations Manager 2005

Description 2/18/2006 5:19:56 PM

Computer Group : Microsoft Operations Manager 2005 Agents

Computer Name	Agent Uptime	System Uptime
CONTOSO\ASPEN	1 days 16h 9m 44s	1 days 16h 10m 5s
CONTOSO\AURORA	2 days 5h 33m 53s	2 days 5h 34m 17s
CONTOSO\BOULDER	6 days 12h 52m 22s	7 days 5h 39m 57s
CONTOSO\CIMMARRON	0 days 3h 11m 45s	0 days 3h 12m 0s
CONTOSO\DALLAS	6 days 14h 42m 52s	6 days 14h 43m 32s
CONTOSO\DILLON	6 days 19h 56m 32s	6 days 19h 57m 37s
CONTOSO\FRISCO	7 days 11h 31m 3s	7 days 11h 32m 21s
CONTOSO\GREELEY	2 days 8h 51m 8s	2 days 8h 51m 35s
CONTOSO\LOVELAND	3 days 18h 57m 33s	3 days 18h 58m 53s
CONTOSO\SNOWMASS	7 days 11h 0m 58s	7 days 11h 2m 29s

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

FIGURE 15.13 Agent Uptime by Computer report.

Microsoft Baseline Security Analyzer Management Pack

Another aspect of monitoring operating systems is knowing whether you are missing security patches. The Microsoft Baseline Security Analyzer (MBSA) Management Pack is designed to scan your servers (Windows 2000 and later) and report on missing security patches and determine security vulnerabilities known to Microsoft. The MBSA management pack also checks for other common security issues including

- Is auto-logon enabled? Auto-logon to a server is a security risk for multiple reasons, among them that the server is automatically logged in to an account that may have elevated security rights, and the user's account and password are stored in plain-text in the registry.
- Is IE enhanced security enabled? Internet Explorer enhanced security should be enabled on all servers to minimize the risk of web pages being accessed that contain viruses.
- Is the Guest account enabled? If the Guest account is not disabled, you have made it much easier for hackers to access your system.

Exposures such as these can result in significant security vulnerabilities and are examples of issues identified by the MBSA management pack. The primary focus of the management pack is actually to assist you in determining what system patches are missing in your server environment. The MBSA management pack installs the MBSA client on your managed systems, downloads updated versions of the MsSecure.cab file, deploys the updated MsSecure.cab to the managed servers, scans the computers, and provides reports on security issues for the monitored systems.

Coupled with Microsoft's Systems Management Server (SMS) or Windows Software Update Services (WSUS), the MBSA management pack provides the ability to detect and alert on missing security patches and notifies you when your servers are configured with known vulnerabilities.

The MBSA MP provides your organization with an effective way to gather and deposit information on Microsoft server security vulnerabilities in a central repository to help assess the significance of any security problems. The MBSA automatically scans for security patch updates for Internet Explorer (IE), Internet Information Server (IIS), SQL Server, and Windows operating systems, and reports on the status of security vulnerabilities.

To utilize the MBSA MP in your MOM 2005 environment, download the Microsoft Baseline Security Analyzer Management Pack. The version of the MBSA supported by the management pack at the time this book was written is 1.2.

After importing the MBSA management pack, you will need to install the MBSA client portion. You should first install the MOM agent on your servers because the agent will copy the MBSA client setup file to the *%ProgramFiles%*\Microsoft Operations Manager 2005\MBSA 1.2 folder. The MBSA client is installed when the MBSA rules are enabled. Further information on implementing the management pack is in the "Configuring the MBSA Management Pack" section later in this chapter.

Setting Up the MBSA Client

By default, MOM does not install the MBSA client or run the security update scan or vulnerability assessment scan on your managed computers. The rule that initiates the MBSA client install and subsequent scans—Microsoft Baseline Security Analyzer \ Baseline Security Analyzer 1.2 \ Mom Agent \ Event Rules \ Run vulnerability and security patch scan—is not enabled by default. Note that its rule group (MOM Agents within the MBSA management pack) is bound to the MOM 2005 Servers, MOM 2005 Agents, MOM 2005 Databases, and MOM 2005 Report Servers computer groups.

Configuring the MBSA Management Pack

Most of the management packs for MOM 2005 are installed by extracting the files and importing them into MOM. The MBSA MP is more complicated, so we provide additional detail to assist with its installation and configuration:

- To use the MBSA management pack you must first designate a server as the file transfer server. This is done by adding the server to the MBSA File Transfer Server computer group, discussed in the "MOM Administrator Console Configurations" section later in this chapter.
- The file transfer server hosts the MsSecure.cab and is configured to automatically download updated versions on a daily basis. The location of the file transfer is configurable under Management Packs \ Rule Groups \ Microsoft Baseline Security Analyzer \ Baseline Security Analyzer 1.2 \ File Transfer Server \ Event Rules within the Download mssecure.cab from http://www.microsoft.com rule. You configure this

rule within the Data Provider tab (the download path varies depending on the version of the Baseline Security Analyzer being used in your environment).

- The MBSA file transfer server requires that IIS 5.0 or later is installed and that it runs Windows 2000 SP3 or later, or Windows 2003. The file transfer server also requires Internet connectivity to download the MsSecure.cab file.

Maintaining the MsSecure.cab File

A manual download of the MsSecure.cab is possible if the file transfer server does not have Internet connectivity, although this is strongly discouraged because you may miss getting timely updates of the cab file. It is imperative that your monitored systems have the latest MsSecure.cab file for MBSA processing against the current set of security patches.

Contents of the MsSecure.cab File

The MsSecure.cab contains the MsSecure.xml—this is the catalog of the security updates. This file changes at least monthly and perhaps more often depending on the frequency of new security patches from Microsoft.

Several steps are associated with creating the file transfer server, which are listed in the following four configuration sections. You can also refer to the Microsoft Baseline Security Analyzer (MBSA) Management Pack Guide for further details.

IIS Configurations

To configure IIS on the file transfer server, complete the following steps:

1. Open the IIS Manager \ Web Sites \ Default Web Site. Right-click on the Default Web Site and choose New \ Virtual Directory.
2. Create an Alias named MBSA and browse to the *%ProgramFiles%*\Microsoft Operations Manager 2005\Downloaded Files*management_group* directory.
3. Select only the Read permission and remove all other permissions. Complete the Virtual Directory Creation Wizard.

Windows Explorer Configurations

You will need to configure security settings for the folder used on the file transfer server to store the downloaded MsSecure.cab files. The procedure for this is as follows:

1. Navigate to the *%ProgramFiles%*\Microsoft Operations Manager 2005\Downloaded Files using the Windows Explorer, right-click on the *management group* directory, and choose Properties.
2. Click on the Security tab and click Add.

3. From the Location tab, choose the File Transfer Server name.
4. Add the IUSR_(*servername*) of the File Transfer Server.
5. On the Security tab, click on the Internet Guest Account and assign the following permissions: Read & Execute, List Folder Contents, and Read. Click OK to close the Properties page.

BITS Configurations

BITS (Background Intelligent Transfer Service) is used to transfer files asynchronously between a client and a Hypertext Transport Protocol (HTTP) Server. BITS is also used by Windows Update and SMS 2003 for file transfers. BITS is bandwidth aware and can restart a transfer at the point that it is interrupted, making it efficient as a file transfer mechanism.

1. On the file transfer server, click on Start, All Programs, Administrative Tools, Services.
2. Right-click on Background Intelligent Transfer Service and choose Properties.
3. Configure the Startup Type to Automatic and start the service if it is not started. Apply your changes and click OK.

MOM Administrator Console Configurations

Using the Administrator console, you will need to specify the name of the file transfer server, enable the rule to run the vulnerability and security patch scan, and indicate the URL of the file transfer server:

1. Go to Management Packs \ Computer Groups, right-click on the MBSA File Transfer Server computer group, and choose Properties. Choose the Included Computers tab and then click Add. Browse to the computer you have designated as the file transfer server, check the box next to the name of the server that you want to add, and click OK; then click OK to close the page.
2. Enable the MBSA management pack rules by opening the Management Packs \ Rule Groups \ Microsoft Baseline Security Analyzer \ Baseline Security Analyzer 1.2 \ MOM Agent \ Event Rules. The Run vulnerability and security patch scan rule installs the MBSA binaries. Right-click on this rule, select Properties, and check the This Rule Is Enabled check box to enable the rule.

   All other MBSA management pack rules are enabled by default. Enabling this rule instructs MOM to install the MBSA on agent computers and run the MBSA scans.
3. Configure the file transfer server address under Administration \ Global Settings. Right-click on the Web Addresses tab on the right-pane and select Properties. On the Custom Web Addresses type in the address of the File Transfer Server Address field in the format of http://*server name*.

Tasks

The MBSA Management Pack includes three tasks that can be initiated using the MOM Operator console:

- Download MsSecure.cab from http://www.microsoft.com.
- Download MsSecure.cab from File Transfer Server.
- Run MBSA Scan.

The MBSA Scan automatically runs daily at 12:30 a.m. You can initiate it on demand and target one or more monitored systems using the Operator console. Selecting the task initiates the Launch Task Wizard, which allows you to customize any of the script task parameters being used. You then select one or more target computers or role instances for the task as shown in Figure 15.14.

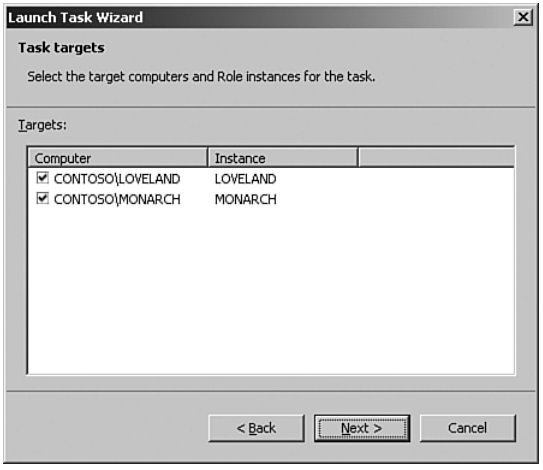


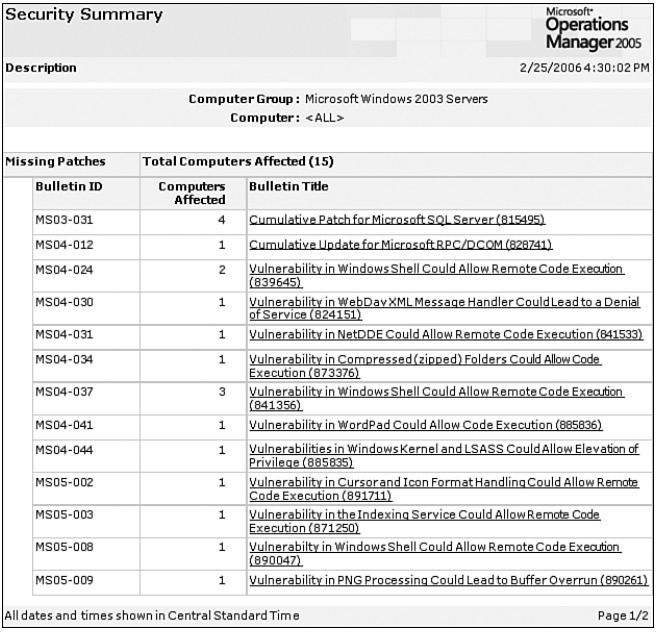
FIGURE 15.14 Select target computers for the task.

Selecting Target Computers

To be able to select target computers, you should first highlight them in the Alerts view prior to selecting the MBSA Scan task.

Reports

The MBSA Management Pack includes two reports: the Security Summary, illustrated in Figure 15.15, and the Security Updates and Vulnerabilities report.



Security Summary

Microsoft Operations Manager 2005

Description 2/25/2006 4:30:02 PM

Computer Group : Microsoft Windows 2003 Servers
Computer : <ALL>

Missing Patches — Total Computers Affected (15)

Bulletin ID	Computers Affected	Bulletin Title
MS03-031	4	Cumulative Patch for Microsoft SQL Server (815495)
MS04-012	1	Cumulative Update for Microsoft RPC/DCOM (828741)
MS04-024	2	Vulnerability in Windows Shell Could Allow Remote Code Execution (839645)
MS04-030	1	Vulnerability in WebDav XML Message Handler Could Lead to a Denial of Service (824151)
MS04-031	1	Vulnerability in NetDDE Could Allow Remote Code Execution (841533)
MS04-034	1	Vulnerability in Compressed (zipped) Folders Could Allow Code Execution (873376)
MS04-037	3	Vulnerability in Windows Shell Could Allow Remote Code Execution (841356)
MS04-041	1	Vulnerability in WordPad Could Allow Code Execution (885836)
MS04-044	1	Vulnerabilities in Windows Kernel and LSASS Could Allow Elevation of Privilege (885835)
MS05-002	1	Vulnerability in Cursor and Icon Format Handling Could Allow Remote Code Execution (891711)
MS05-003	1	Vulnerability in the Indexing Service Could Allow Remote Code Execution (871250)
MS05-008	1	Vulnerabilty in Windows Shell Could Allow Remote Code Execution (890047)
MS05-009	1	Vulnerability in PNG Processing Could Lead to Buffer Overrun (890261)

All dates and times shown in Central Standard Time Page 1/2

FIGURE 15.15 Microsoft Baseline Security Analyzer security summary.

How the MBSA Management Pack Works

Now that the MBSA Management Pack is configured, let's look at how it works. The File Transfer server downloads the latest MsSecure.cab every morning by default at 4:00 a.m. to the *%ProgramFiles%*\Microsoft operations manager 2005\Downloaded Files\ <*management group name*>\ folder. Clients will transfer the MsSecure.cab from this location (also known as the MBSA virtual folder) locally to the equivalent folder at 5:00 a.m. daily by default. Each client machine then runs the MBSA Install and Run script at 12:30 a.m. the following day.

The Install and Run script installs the MBSA client if necessary and runs the mbsacli.exe command, using the current MsSecure.xml from the MsSecure.cab downloaded from the File Transfer server. The MBSA compares the security patches listed in the MsSecure.xml file to what is already installed on the client. In addition to missing security patches, the MBSA checks for known security vulnerabilities for the operating system, IIS, Internet Explorer, and SQL Server.

The information gathered by this scan is encapsulated in internal MOM events and passed back to the MOM server, where event rules act on the events generated by the script, creating alerts as necessary. The event data is also the basis for the MBSA reports. The MBSA MP provides an effective method to report on the status of patches within your environment, a necessary requirement when monitoring the security of your operating system environment.

Other Management Packs to Manage the Operating System

Earlier sections of this chapter focused on the stability, performance, and security aspects of monitoring operating systems. After these criteria are met we can focus on the functionality the system provides. In this section of the chapter we will discuss additional management packs associated with services used as part of the Windows operating system. These include the Availability Reporting, Server Performance Advisor, Terminal Server 2005, Virtual Server 2005, Distributed File System (DFS), Network Load Balancing (NLB), Print Server, Routing and Remote Access Service (RRAS), Server Clusters, and Windows System Resource Manager (WSRM) management packs.

Availability Reporting Management Pack

The stability of your operating systems can be measured by the amount of time they are available. Servers experiencing unexpected outages can be identified with the Microsoft Availability Reporting Management Pack. This MP tracks the availability of your servers over a period of time and provides reports to track trends. Reports from the management pack can be used to identify causes of both planned and unplanned downtime and take preemptive actions that may decrease future downtime.

Most management packs are installed by extracting files from a package and importing them into MOM. The Availability Reporting MP is somewhat more complicated, so we provide additional information to assist in installing and configuring the management pack.

To install the management pack, follow the standard process to download the management pack by extracting the files and importing the management pack and its included report. Extracting the management pack also gives you two additional MSIs (Microsoft Installer files):

- MOM-MRAS.msi—The MOM-MRAS.msi needs to run on the MOM Reporting server system hosting the SystemCenterReporting database. It extracts into the *%ProgramFiles%*\Microsoft Reliability Analysis Reporting\MomReliabilityAnalysisReporting directory by default. This file is used to install the Availability Reporting SQL Reporting Server components; it installs the SQL backend tables and the DTS job required for the Availability reports.
- MRAS_MP_UI.msi—The MRAS_MP_UI.msi installs the Availability Reporting Microsoft Management Console (MMC) snap-in.

The MRAS_MP_UI.msi snap-in can be added with the following steps:

1. Click Run on the Start menu and type **MMC**.
2. Open the File menu and select Add/Remove Snap-in.
3. In the Add Standalone Snap-in screen, select the Microsoft Availability Reporting Console and click Add.
4. You can save this console for future use by selecting the File tab and choosing Save As. Save the MMC as Availability Reporting.msc to make it easy to identify.

The Availability Reporting Management Pack creates a number of rule groups but does not link any computer groups to the rule groups, which is required for the rules to function. To link the groups, open the Administrator console under Management Packs \ Rule Groups \ Microsoft Availability Reporting Management Pack for Microsoft Operations Manager 2005 \ Application Events. Right-click on Application Events and click Associate with Computer Group. Depending on which servers you want the management pack to monitor, you will want to choose either a custom computer group or the Microsoft Windows Servers computer group.

Each rule group must be linked to a computer group appropriate to your organization. Documentation in the Availability Reporting Management Pack Guide states that computer groups should be linked to rule groups as shown in Table 15.1.

TABLE 15.1 Rule Groups and Computer Groups for the Availability Reporting MP recommended by the Management Pack Guide

Rule Group	Computer Group
Microsoft Availability Reporting Management Pack for Microsoft Operations Manager 2005	Microsoft Windows 2000 and 2003 Servers
Application Events	Microsoft Windows 2000 and 2003 Servers
Directory Services	Windows 2003 Domain Controllers Windows 2000 Domain Controllers
Installer Events	Microsoft Windows 2000 and 2003 Servers
Microsoft Exchange Events	Microsoft Exchange Installed Computers
Microsoft SQL Server Events	Microsoft SQL Server 2000 Microsoft SQL Server 2005
System Events	Microsoft Windows 2000 and 2003 Servers

Unfortunately linking the rule groups to the computer groups listed in Table 15.1 in earlier releases of the Availability Reporting MP did not generate any reports. As Microsoft discusses in support document #914989 (http://support.microsoft.com/kb/914989/) the solution was to associate the computer groups with the top-level rule group as shown in Table 15.2. Microsoft released a substantial update to the Availability Reporting MP at the end of August 2006. The updated version appears to have resolved the computer group issues so Table 15-1 does in fact represent the correct mapping.

TABLE 15.2 Rule Groups and Computer Groups for the Availability Reporting MP recommended by Microsoft (KB 914989)

Rule Group	Computer Group
Microsoft Availability Reporting	Microsoft Windows Servers
Management Pack for Microsoft	Windows 2003 Domain Controllers
Operations Manager 2005	Microsoft Exchange Installed Computers
	Microsoft Exchange Installed Computers
	Microsoft SQL Server 2000

Implementing the Availability Reporting MP

When we initially tested this management pack we had a great amount of difficulty generating reports. First, we recommend patience. A few things have to happen for this management pack to reach the point where any reports are available.

After linking the computer groups to the rule groups and creating the reports within the Availability Reporting MMC (shown in Figure 15.16), the SystemCenterDtsPackageTask has to run successfully to archive data into the reporting database (this is a nightly scheduled task); then the ReliabilityAnalysisReporting scheduled task also must run successfully. You may also want to view document #918119 at http://support.microsoft.com/kb/918119/.

No reports are available when the Availability Reporting Management Pack is initially installed. The MMC snap-in is used to create the reports you will use in your own particular environment.

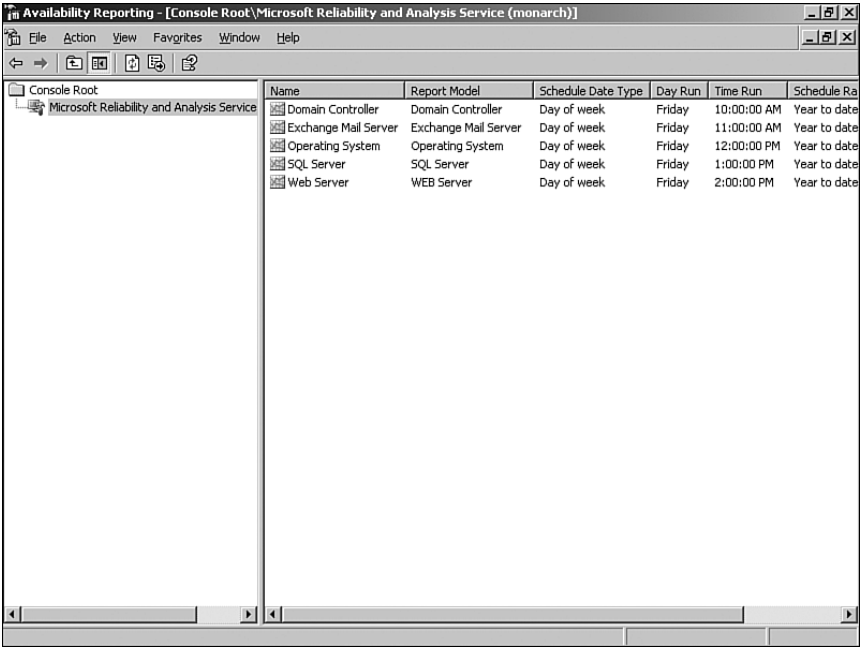
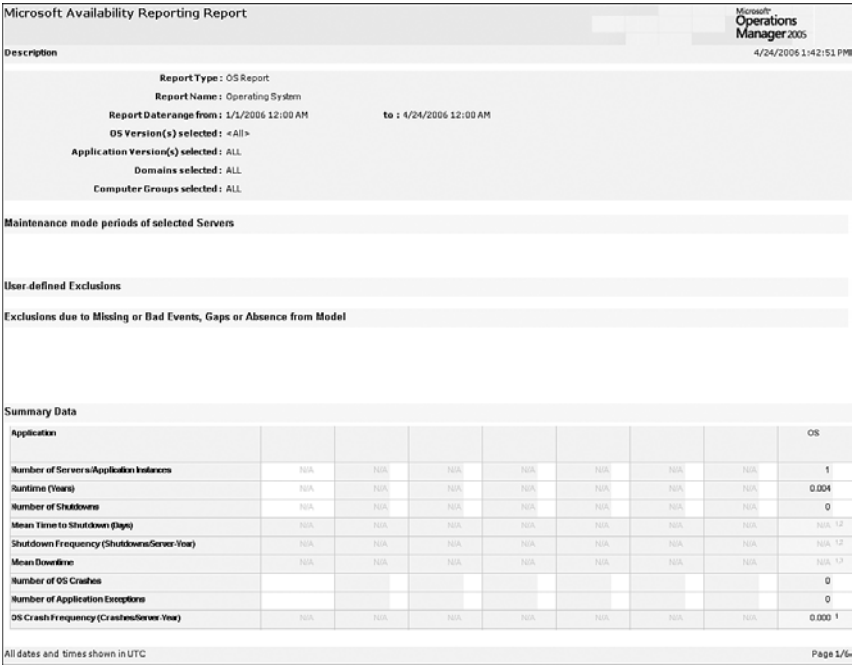


FIGURE 15.16 Availability Reporting MMC with multiple reports scheduled.

Our recommended process to create reports is first link the groups, next create the reports, and then let the archiving and reliability analysis jobs run for a few days before taking any further actions. When the management pack is fully functional it creates reports such as the one shown in Figure 15.17, which shows a subsection of the Operating System availability report. The report is available in the Reporting console under Microsoft Operations Manager Reporting \ Microsoft Availability Reporting Management Pack for Microsoft Operations Manager 2005 \ Microsoft Availability Reporting Report.



Microsoft Availability Reporting Report

Microsoft Operations Manager 2005

Description 4/24/2006 1:42:51 PM

Report Type : OS Report
Report Name : Operating System
Report Daterange from : 1/1/2006 12:00 AM to : 4/24/2006 12:00 AM
OS Version(s) selected : <All>
Application Version(s) selected : ALL
Domains selected : ALL
Computer Groups selected : ALL

Maintenance mode periods of selected Servers

User-defined Exclusions

Exclusions due to Missing or Bad Events, Gaps or Absence from Model

Summary Data

Application								OS
Number of Servers/Application Instances	N/A	N/A	N/A	N/A	N/A	N/A	N/A	1
Runtime (Years)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0.004
Number of Shutdowns	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0
Mean Time to Shutdown (Days)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A [1,2]
Shutdown Frequency (Shutdowns/Server-Year)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A [1,2]
Mean Downtime	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A [1,2]
Number of OS Crashes								0
Number of Application Exceptions								0
OS Crash Frequency (Crashes/Server-Year)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0.000 [1]

All dates and times shown in UTC Page 1/6

FIGURE 15.17 The Microsoft Availability Reporting operating system report.

A Last Resort to Get the Availability Reports Working

If attaching your reports and waiting the required amount of time does not work, as a last resort, Justin Harter (a MOM MVP [Most Valuable Professional]) MSN's blog provides a fix we used to get our reports functional. The steps are available at http://spaces.msn.com/jharter/blog/cns!39CE28DB5474A6C7!264.entry. (This reference URL is also available within Appendix E.)

Please note that thisfix was created prior to the version of the Availability reports released in August 2006.

The reporting functionality provided with the Availability Reporting Management Pack can help you determine which systems are not meeting their availability requirements and work to provide increased stability for the operating systems in your environment.

Server 2003 Performance Advisor

For Windows Server 2003 systems, another monitoring-related management pack is available. The Server 2003 Performance Advisor Management Pack gathers performance information and provides reports that can be used to analyze potential performance bottlenecks.

The Server Performance Advisor Management Pack (or SPA for short) is designed to provide reports for roles such as Active Directory File, DNS, IIS and (Operating) System

Overview. By default, the SPA management pack only collects data and provides reporting information. Three performance rules disabled by default can be activated to provide alerting on potential error conditions:

- Active Directory Investigate CPU Busy
- System Overview Investigate CPU Busy
- IIS Investigate CPU Busy

Enabling these rules will provide alerting capability.

The SPA management pack is deployed as other standard management packs are, by importing the management pack. The SPA management pack requires the SPA program. To download the SPA utility, access the Microsoft downloads website at http://download.microsoft.com and search for "SPA."

The SPA program must be deployed to systems you want to analyze with the Server 2003 Performance Advisor. The management pack is used to gather the data distributed to servers running the SPA utility.

The SPA MP pack has tasks to start or stop the jobs that collect data on Active Directory, System Overview, and IIS. The management pack does not include reports, which means no reports are available from the MOM Reporting console. The reports for the Server 2003 Performance Advisor are available as part of the SPA user interface, shown in Figure 15.18.

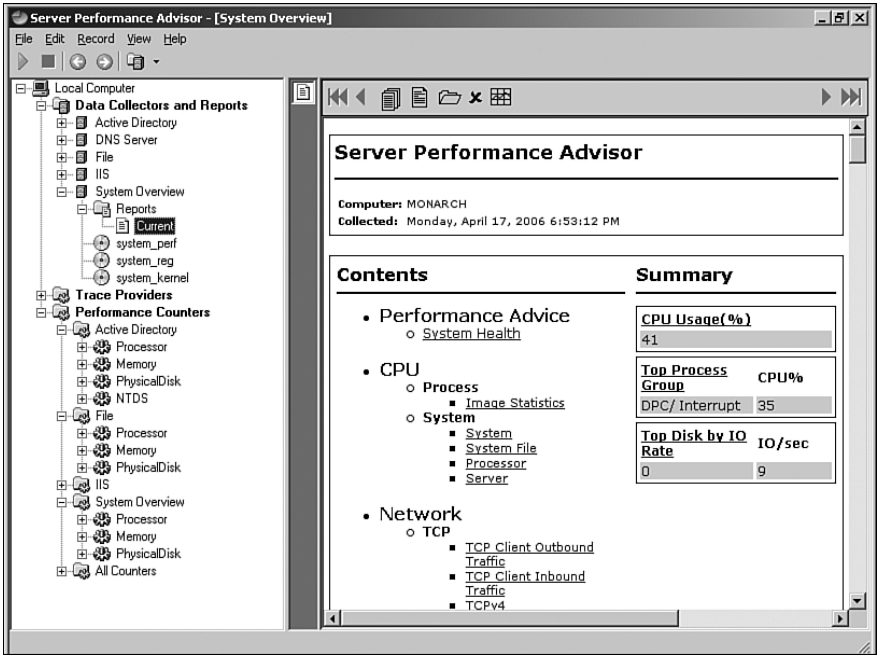


FIGURE 15.18 Server performance advisor.

This interface includes multiple reports including the general System Overview report (a subset of which is shown in Figure 15.19).

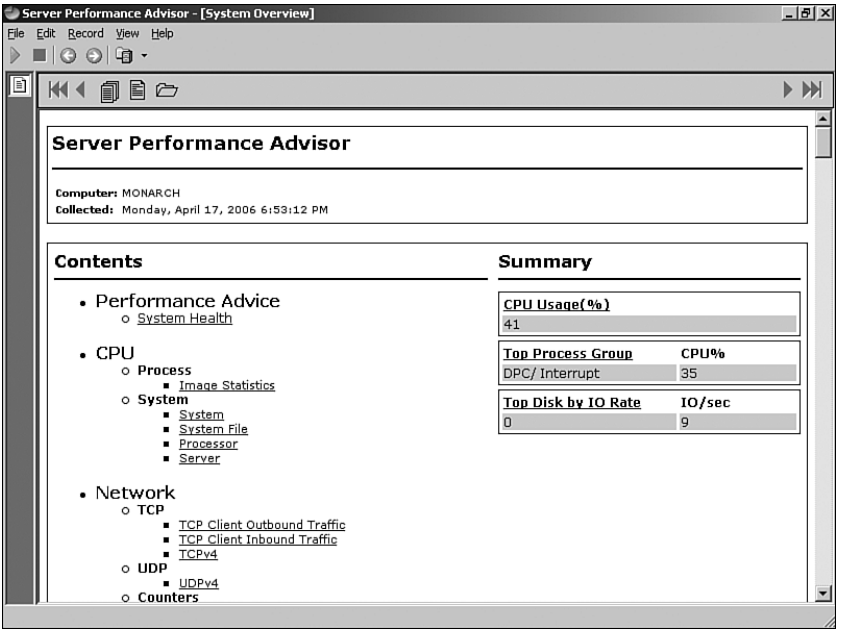


FIGURE 15.19 Server Performance Advisor Overview report.

Sometimes seeing the same information displayed in different ways can help provide new insight for resolving an issue. The Server 2003 Performance Management Pack is an additional tool to assist in identifying and resolving bottlenecks within Windows 2003–based operating systems, taking a different approach to examine the same information.

Terminal Server

Terminal services are tightly coupled with Windows. It is a critical piece of the functionality the operating system is expected to provide and has been core Windows technology since the release of Windows 2000. Terminal services provide two primary functions: remote administration and application sharing. Many organizations with Windows servers use terminal server functionality to provide remote connectivity for administration purposes. Some organizations also use terminal services to share applications or desktop environments to users often in physically remote locations.

To support terminal server monitoring functionality for remote administration or application sharing, Microsoft provides the Terminal Server Management Pack for Microsoft Operations Manager 2005. This management pack is available for download from the Management Pack Catalog website discussed earlier in this chapter (http://go.microsoft.com/fwlink/?linkid=43970). A management pack guide is also available and included with the management pack download package.

The Terminal Server Management Pack can monitor terminal server functionality and report on issues impacting that functionality. Items being monitored include availability of the terminal server services, client connection failures, printer redirection issues, and the health of Terminal Server Licensing.

The management pack also gathers metrics used to provide historical tracking related to the utilization of terminal services within your environment. Tasks are included to query sessions, users, and processes as well as to enable, disable, or query whether users are allowed to log on to the terminal server.

As terminal services have evolved into a core piece of the Windows Server System, the need to monitor them has also increased. The Terminal Server Management Pack provides you with the information needed to effectively do so.

Virtual Server 2005

Virtualization technologies are being increasingly embraced by the technology community. Virtualization allows a single physical system (referred to as the *host* or *virtual server*) to run multiple additional operating systems (referred to as *guests*, or *virtual machines*). Microsoft provides two virtualization products: Virtual PC and Virtual Server. Virtual PC is designed to provide a workstation-level virtualization, whereas Virtual Server is designed to provide server-level virtualization.

Virtualization can provide significant benefits to an organization by providing server consolidation. Virtualization is most often used to gather smaller, seldom-utilized applications running on a variety of platforms and bring them together onto a single shared physical server, or to provide development/testing environments. Production environments can also be run on virtualization solutions such as Virtual Server 2005. Microsoft offers Virtual Server 2005 R2 at no charge and we expect that the market share for Virtual Server will increase quickly.

Virtual Server 2005 R2 Management Pack

The Microsoft Virtual Server 2005 R2 Management Pack is designed specifically for Virtual Server 2005 R2. The management pack builds on the Virtual Server 2005 management pack and adds new functionality including a new diagram view, a virtualization candidates report, and identification of the host and guest operating systems for a virtual machine.

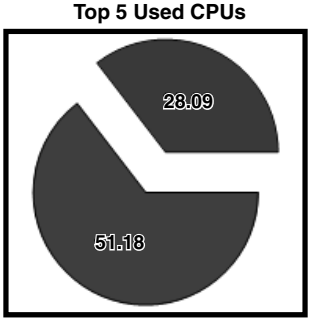
Several terms need to be defined to discuss the Virtual Server 2005 management pack. These include

- *Virtual server*—The physical machine hosting virtual machines
- *Virtual machine*—A hardware-emulated platform allowing multiple operating systems to exist with each in its own isolated software partition
- *Virtual network*—An emulation of a physical network
- *Virtual hard disk*—A single file that emulates a hard drive

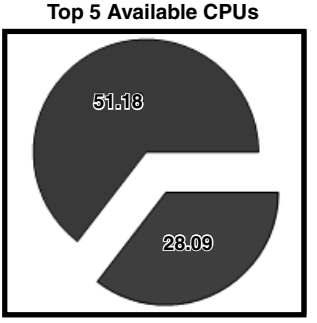
The management pack monitors the availability, health, and performance of Microsoft virtual servers and virtual machines in your environment, includes tasks to perform common virtual server related functions, and reports information about the configuration and performance of virtual servers in your environment.

Tasks in this management pack start, stop, save state, resume, reset, or pause the virtual machine. There are also tasks that apply on the virtual server level to start or stop the virtual server itself.

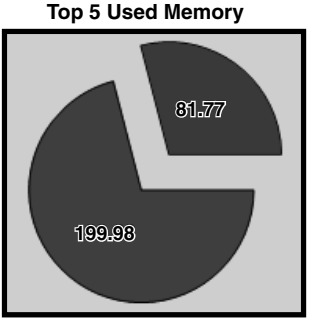
Reports provide both configuration and historical performance information for the virtual servers within your environment. Three reports are included to track performance trending with details on CPU utilization, disk space used, and RAM used over time. Figure 15.20 shows the All Virtual Servers Report, which graphs information about CPU, memory, and disk usage.



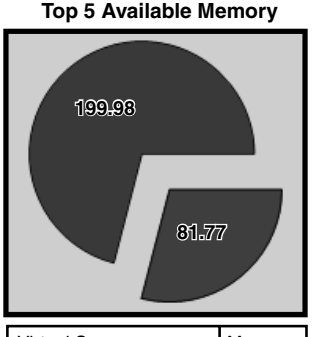
Virtual Server Name	% CPU Usage
CONTOSO\MONARCH	51.18
CONTOSO\AURORA	28.09



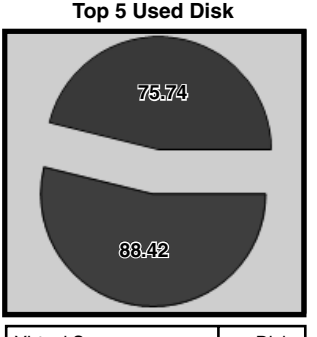
Virtual Server Name	% CPU Usage
CONTOSO\MONARCH	28.09
CONTOSO\AURORA	51.18



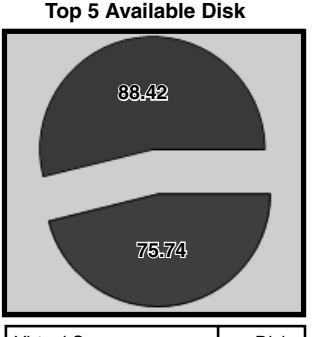
Virtual Server Name	Memory Usage (MB)
CONTOSO\MONARCH	199.98
CONTOSO\AURORA	81.77



Virtual Server Name	Memory Usage (MB)
CONTOSO\MONARCH	81.77
CONTOSO\AURORA	199.98



Virtual Server Name	Disk Usage (%)
CONTOSO\MONARCH	88.42
CONTOSO\AURORA	75.74



Virtual Server Name	Disk Usage (%)
CONTOSO\MONARCH	75.74
CONTOSO\AURORA	88.42

FIGURE 15.20 All Virtual Servers report.

If your server environment uses Virtual Server 2005, the Virtual Server Management Pack will help meet the requirements of managing your operating systems by providing information to monitor the virtual server aspects of your environment.

Monitoring VMWare Servers

If you use VMWare rather than Virtual Server, eXc software provides a management pack to monitor VMWare server systems. Information on this management pack is available at the Management Pack Catalog (http://go.microsoft.com/fwlink/?linkid=43970).

Windows DFS Service 2000, 2003

File sharing is a core part of operating system functionality. Windows DFS provides a way to simplify how users find files stored on the systems within their network. DFS is a method to share folders located on different servers and present them in a virtual tree of folders, known as a *namespace*. The namespace allows users to locate files through a single folder structure regardless of which server files actually are stored on. A namespace can consist of multiple servers with redundant shares, which provide higher availability to the files stored within the namespace. For example, within our Contoso domain we maintain copies of all software used for installation on two file and print servers (named Montrose and Vail). Both servers can be configured with DFS and be part of a single namespace so that if one server should fail, the other server provides redundant access to the files.

The Windows DFS Service Management Pack monitors the health and performance of DFS functionality and can monitor a client's capability to access DFS paths through client-side monitoring. This management pack includes tasks and reports to assist with managing and monitoring the DFS functionality.

Several terms need to be defined to discuss the DFS management pack. These include the following:

- *DFS namespace*—A view of shared folders on different servers that starts with a root that maps to one or more root targets.
- *DFS server*—A server that runs DFS and is hosting a DFS root.
- *DFS client*—A computer that uses DFS to access the shares on the network.
- *DFS root*—Maps one or more root targets to a shared folder on a separate server.
- *Root Target*—A server that hosts a DFS namespace. A stand-alone DFS root can have only one root target, but a domain-based DFS root can have multiple root targets.

By default, client-side monitoring is not activated as part of the management pack installation. To activate client-side monitoring, perform the following configuration steps:

1. Add the system(s) that you want to perform client-side monitoring to the Microsoft Windows Distributed File System Client Side Monitoring computer group.

2. On the rule's Response tab configure the RootLink script parameter with a list of the DFS paths that the system should test for availability. This rule is located under Management Packs \ Rule Groups \ Microsoft Windows Distributed File Systems \ Windows (All Versions) \ Client Side Monitoring \ Event Rules \ *<Windows version>* \ DFS client side root and link destination availability health check.

Overrides can be used to allow some of the systems to connect to DFS paths that are different from the ones specified in the RootLink parameter.

The DFS management pack provides the information needed to monitor and manage file sharing functionality within your managed operating systems.

Windows Network Load Balancing

As discussed in Chapter 10, "Complex and High Performance Configurations," Network Load Balancing (NLB) is often used to provide load balancing and redundancy for applications not requiring shared data (such as web servers). To monitor this capability, you can use the Windows Network Load Balancing Management Pack.

The NLB management pack detects critical events related to NLB clusters to provide alerts and automated responses. Event rules are provided for configuration errors such as invalid IP configurations. Events associated with runtime events reported by the driver include the cluster mode started, stopped, suspended, or resumed; resource allocation problems; and authentication issues.

The NLB MP works through responding to a variety of events within the Windows System event log from the WLBS source (Windows Load Balancing Service). Critical errors found from these rules will generate an alert to the Cluster Administrators notification group.

Although the NLB management pack may not have as much functionality as some of the others (the current version has no tasks or reports included because it is a MOM 2000 management pack), if you use NLB within your environment you will want to be aware of the status of your NLB components when monitoring your Windows operating systems.

Windows Print Server

Print server functionality is an important piece of functionality expected in server operating systems. The Print Server Management Pack monitors the availability, health, and performance of Windows print servers.

The management pack checks the Windows System event log for various items with the source of Print and also tracks performance metrics that can be seen within the Printers report. The Windows Print Server MP also provides a report (located under Microsoft Windows Print Server) that gives a summary of the printers that are shared. This report is shown in Figure 15.21.

The Print Server Management Pack provides another piece to the puzzle of using MOM 2005 to manage your operating systems.

Printers

Microsoft Operations Manager 2005

Description

4/20/2006 2:29:08 PM

Computer Group : Microsoft Operations Manager 2005 Agents
Server : <ALL>

Server	Printer Name	Description	Location	Share	Driver Name
CONTOSO\CIMMARRON					
	EPrinter			HP2500CS	HP 2500C Series PS3
CONTOSO\LONGMONT					
	HPLJ4KPCL6			HPLJ4KPCL6	HP LaserJet 4000 Series PCL 6
	HP LaserJet 4000 Series PCL 6			HPLaserJ	HP LaserJet 4000 Series PCL 6
CONTOSO\MONTROSE					
	HP LaserJet 4000 Series PCL 6			HPLaserJ	HP LaserJet 4000 Series PCL 6
CONTOSO\WAIL					
	PSSTMNT-PRP62	Cycle 1,2 &3 - PT 04	Print Services	PSSTMNT-PRP62	Xerox DT6100 PS3 v2.0

FIGURE 15.21 Sample Printers report.

Windows RRAS

Another type of functionality often utilized with Windows Server is the Routing and Remote Access Service (RRAS). RRAS provides connectivity to network resources from remote locations using either dial-up or Virtual Private Network (VPN) connectivity.

The Windows RRAS management pack is a MOM 2000 management pack, which means it does not have tasks or reports. It does, however, give you a method to monitor RRAS functionality by monitoring the availability, health, and configurations used by both Routing and Remote Access and the Remote Access Connection Manager service.

If users connect to your network remotely and you use RRAS to provide this capability, this management pack can assist in monitoring this important aspect of the operating system.

Windows Server Clusters

As discussed in Chapter 10, the Windows Server Clusters (MSCS) management pack monitors the functionality of clustered servers within your environment. Server clusters are often used on database configurations or systems that share data between the systems within the cluster. This is different from NLB clusters that do not share data.

Several terms need to be defined to discuss the Server Cluster management pack, including

- *Cluster*—A group of servers that work together as a single system to provide high-availability of the resources that they manage.
- *Cluster nodes*—The servers that are members of the cluster.
- *Cluster groups*—The units that can fail over from one cluster node to another. Groups are always owned by only one node at any point in time.
- *Cluster resources*—These belong to cluster groups. Types of resources include but are not limited to physical disks, IP addresses, Network Names, and so on.

The Windows Server Clusters Management Pack monitors the availability and health of the various components of the Microsoft Cluster solution. This includes the server cluster, cluster nodes, cluster groups, and cluster resources. This management pack includes tasks that perform a variety of functions, including opening the cluster administrator, displaying the cluster properties, pausing/resuming cluster nodes and stopping/starting the cluster service. Reports are also included in the management pack giving details on cluster configuration as well as cluster servers and nodes.

From the Administrator console, you can see clustered nodes within the environment under Administration \ Computers \ Windows Server Cluster Computers, as shown in Figure 15.22.

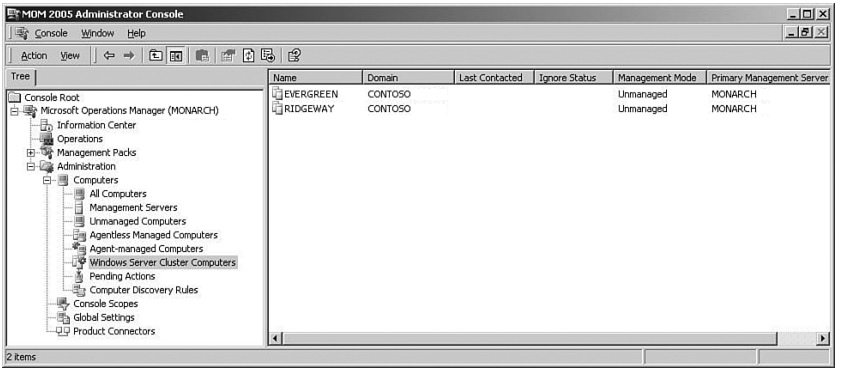


FIGURE 15.22 Windows Server Cluster Computers in the Administrator console.

You can quickly view the state of the cluster using the MOM Operator console, as shown in Figure 15.23. There is a Cluster state view column indicating the state of the cluster functionality and also whether the server is an active node—shown by a green, yellow, or red check box for the server.

This State view can also be highlighted to provide information about the subcomponents within the cluster. Figure 15.24 shows the subcomponents of the cluster (Disk, IP, Name, Online, Service) and their current status.

If you are using Windows clusters within your environment the Windows Server Clusters MP provides another tool to assist in monitoring your operating systems. Clustered resources usually require the highest level of availability. This management pack helps diagnose and resolve issues quickly to maintain the high levels of uptime required by clusters.

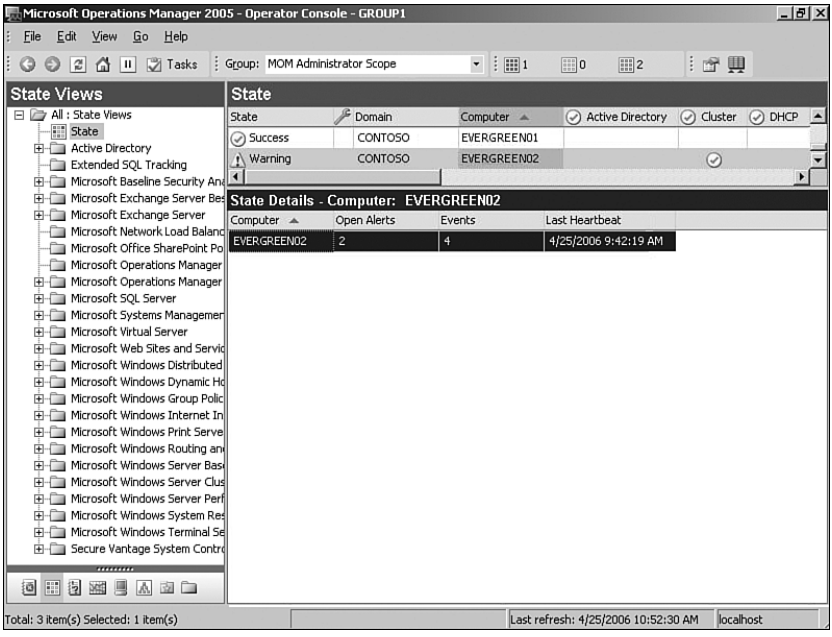


FIGURE 15.23 Windows cluster status in the Operator console.

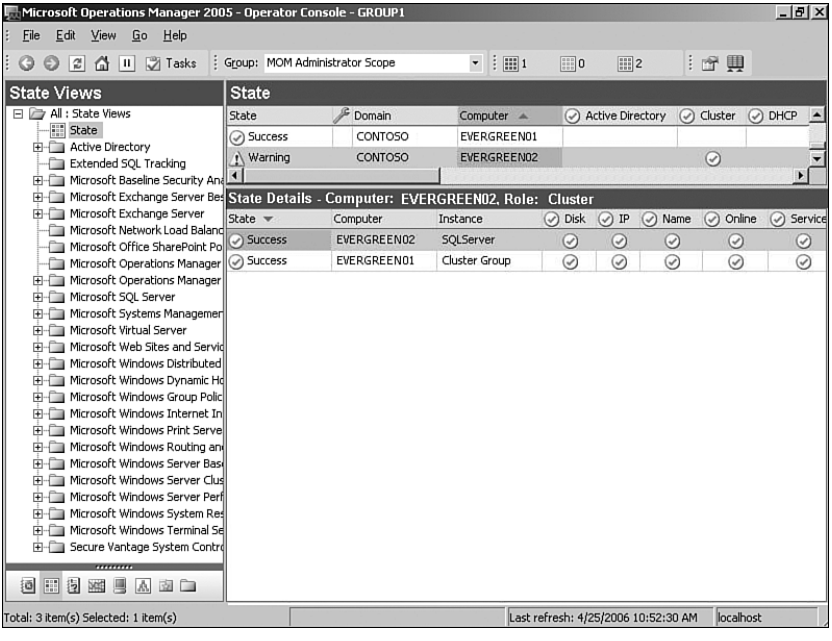


FIGURE 15.24 Windows cluster subcomponent status in the Operator console.

Windows System Resource Manager 2003

The Windows System Resource Manager (WSRM) is a new component for Windows Server 2003 and provides management of processor and memory resources among applications or terminal server users. Processor time and memory can be configured to prioritize applications based on your business requirements. You can use WSRM to run multiple applications on a server and prevent them from using more than the amount of CPU and memory you allocate. WSRM uses policies that can be applied using a date or time schedule. For example, policies could be created to focus resources on real-time applications used during the business day with after-hours resources shifted to batch-processing applications.

WSRM also provides an accounting feature allowing administrators to create reports for resource utilization, track service level agreements, or bill for resources used. WSRM is available on the Windows 2003 Enterprise and Datacenter editions and can be downloaded from http://www.microsoft.com/technet/downloads/winsrvr/wsrm.mspx.

WSRM is administered with an MMC snap-in, shown in Figure 15.25. This interface also provides a resource monitoring graph that can be useful to track WSRM metrics.

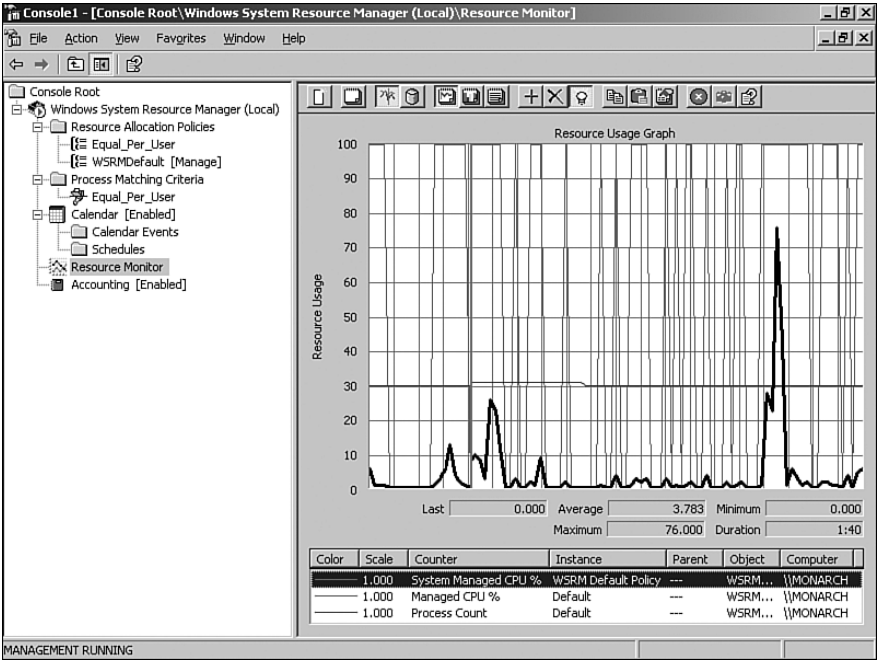


FIGURE 15.25 WSRM Resource Monitor.

The WSRM management pack is designed to monitor the functionality of WSRM and monitor WSRM specific performance counters. The management pack monitors application events with a source of WSRM to alert on conditions such as when issues occur that

impact its functionality (database issues, service errors, and so on). It also monitors WSRM-specific counters such as the Target Managed CPU and Actual Managed CPU.

If you are currently using WSRM in your environment planning to in the future, the WSRM management pack will assist in monitoring this important aspect of Windows Server 2003.

Third-Party Tools

Although Microsoft provides a number of management packs that assist with monitoring your Windows-based operating systems, some excellent third-party management packs also can be used to increase your ability to monitor your Windows systems using MOM 2005.

PinPoint

The PinPoint product by RTO Software provides a bidirectional connector between MOM 2005 and the PinPoint application. The application is designed to monitor mission-critical Windows server applications and help those applications meet their Service Level Agreements (SLAs). PinPoint's focus is to monitor and prevent application issues before they impact the end-users of the application. Integration with MOM increases the functionality of both products. Linking together MOM 2005 and PinPoint provides benefits primarily by reducing the number of situations where MOM may generate alerts for items that do not impact an application's SLAs. PinPoint's focus is to monitor whether an application is meeting its service levels. For example, say that four web servers are used for a web-based application. If one of the four goes offline and the remaining three servers can meet your service level requirements, you can use PinPoint to determine whether the outage is important enough to page support personnel during off-hours.

Another area where MOM and PinPoint work together is PinPoint's capability to determine the root cause of issues through its "replay" functionality. Should a server die outside business hours, support personnel can later replay the metrics gathered at night to assist in debugging why the server crashed.

PinPoint's information can be integrated into the MOM Administrator console using the bidirectional connector, and all counters gathered by PinPoint are available as standard performance monitor counters that can be exposed as long as the PinPoint agent is installed on the monitored system.

With the PinPoint connector you can receive alerts within the Operator console and access the PinPoint reports for that alert. Figure 15.26 shows an example where the Cortez server has a PinPoint alert generated for % Processor Time Exceeded Critical Threshold and provides a link to the PinPoint report, which gives additional data.

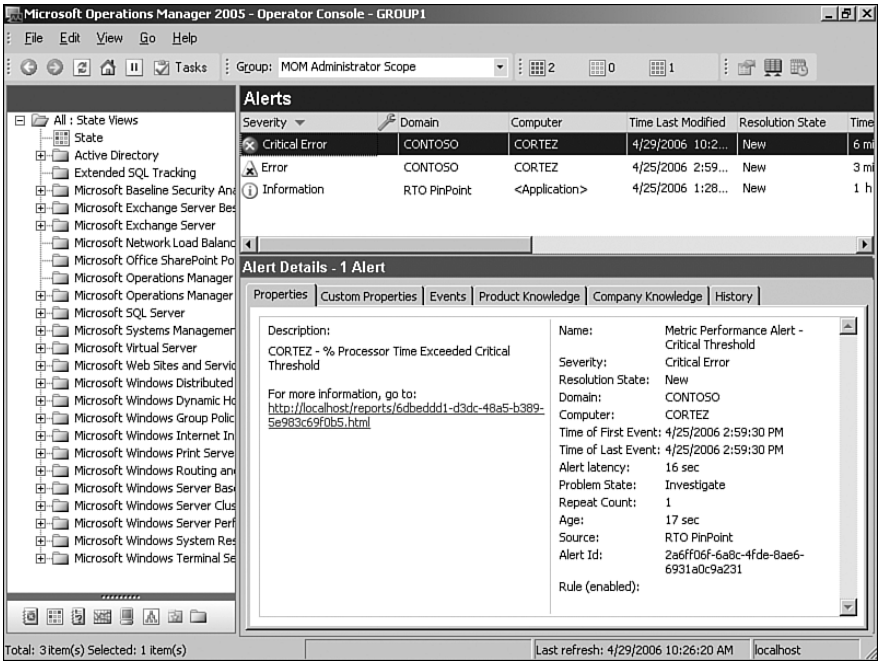


FIGURE 15.26 PinPoint alert in the MOM Operator console.

Quest Troubleshooting Management Pack for Windows (Spotlight)

Quest Software provides several products that can be used to complement your MOM 2005 environment. The Spotlight line of products includes tools for Active Directory, Exchange, SQL Server, and Windows. On the Management Pack Catalog page (http://go.microsoft.com/fwlink/?linkid=43970), this management pack is listed as the Troubleshooting Management Pack for Windows. From this link you can get further information or download an evaluation copy of the product. To evaluate the product, register and download the Spotlight on Windows.

Figure 15.27 shows the Spotlight on Windows' main page, which gives an overall picture of the server health including the system, network, event logs, CPU, memory, paging files, and disk.

The Spotlight for Windows allows you to view on a single screen the detailed technical status of a Windows-based server. You can gather even more information by drilling down into the various sections of the interface. The Quest Spotlight for Windows enhances the ability to quickly identify and resolve issues especially when they are related to the performance of operating systems.

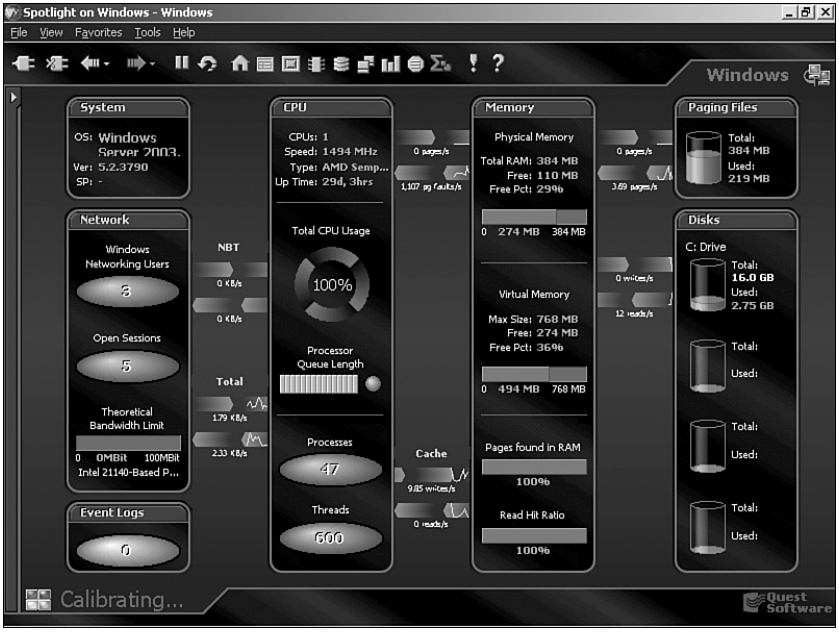


FIGURE 15.27 Quest Spotlight for Windows.

Auditing and Security Tracking with the System Controls Management Pack

SecureVantage Technologies' System Controls Management Pack (SCMP) is designed to extend MOM 2005's capabilities to provide best practices for regulations such as the Federal Information Security Management Act (FISMA), Gramm-Leach-Bliley Act (GLBA), and Sarbanes-Oxley Act (SOXA), which require auditing of IT assets and specific controls. To facilitate this type of functionality, the SCMP includes services that focus on the following areas: account management, auditing integrity, object access, logon activity, policy changes, and privilege use.

The SCMP is an excellent example of how third-party management packs can be created to provide additional functionality within MOM while being implemented as a standard MOM management pack (using the procedures of importing the .akm file and/or the report definitions). The SCMP management pack provides a variety of different views that can be used to analyze the information provided within the MOM Operator console.

The SCMP not only reports on events, it provides notification when security-related items occur. Figure 15.28 shows an example where a warning has been generated in the Operator console that the system log has been cleared.

The SCMP also includes tasks and many reports that provide information on items such as data access failures, group account management, logon failures, user account changes, and password change history, illustrated in Figure 15.29.

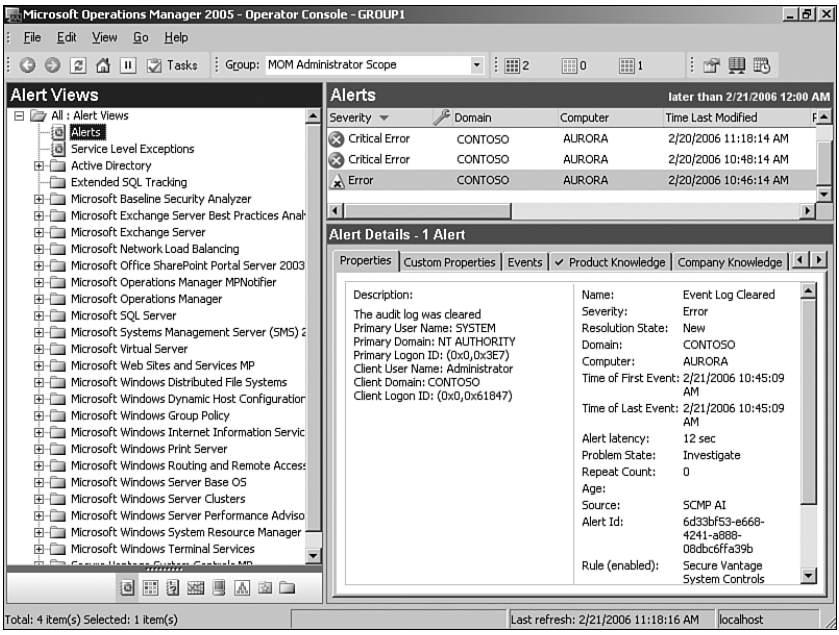


FIGURE 15.28 System log cleared warning.

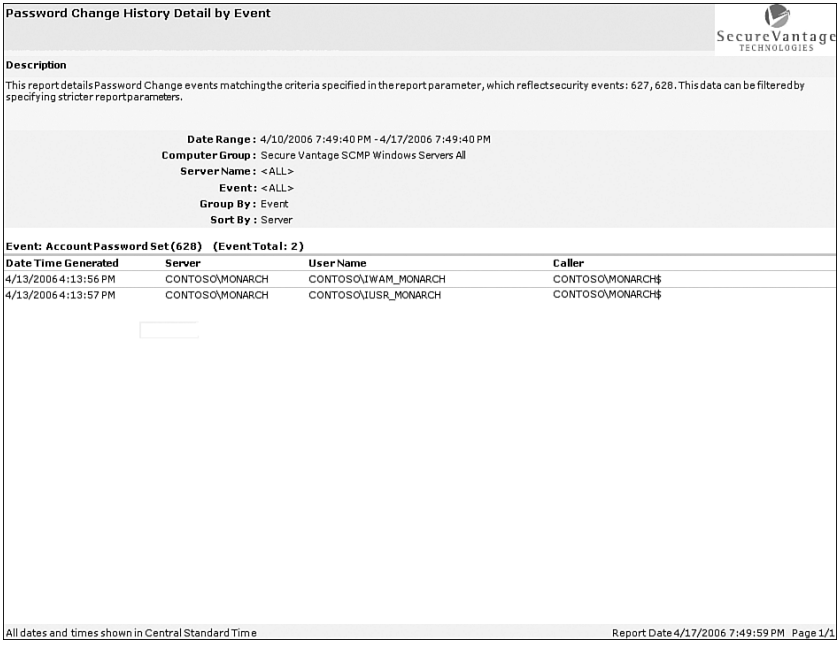


FIGURE 15.29 Password Change History Detail report.

You may want to assess the SCMP especially if your organization is required to abide by regulations such as FISMA, GLBA, or SOXA, and uses MOM 2005. Additional information on the SCMP is available at the SecureVantage website at http://www.securevantage.com/ProductsSCMP.html.

Summary

This chapter focused on the various management packs available to assist in managing the Windows operating systems. We discussed management packs from Microsoft as well as third-party solutions that can supplement Microsoft's offerings. In the next chapter we will build on our operating system foundation as we discuss managing directory services with MOM 2005.

This page intentionally left blank

CHAPTER 16

Managing Directory Services

IN THIS CHAPTER

- Using Management Packs to Manage Directory Services
- Active Directory Management Pack
- Other Management Packs for Directory Services
- Third-Party Tools

Are your company's directory services working correctly? A typical reaction to this question is something to the effect of "The Help Desk isn't getting calls so things must be okay." Unfortunately, far more is involved than calls to a help desk when determining whether directory services are functioning properly.

A healthy directory service entails that replication is occurring in a timely manner, clients are connecting and authenticating, and the base services used by Active Directory (AD) are working correctly. AD is a distributed repository of information about the objects in your environment—such as users, computers, printers, and applications. The directory provides integrated management and secure access to network resources. Authenticating users and services, discovering resources, group policies, and applications such as Exchange Server depend on proper functioning of Active Directory, and Active Directory is critical when users and systems require directory services functionality in a Windows server environment.

AD failures can prevent users from successfully accessing email, slow user authentication, or even prevent logging in to computer systems. Active Directory can have additional complexities because it is a distributed system, and distributed systems can experience unexpected issues. The fact that Active Directory is performing well at one location does not ensure that users elsewhere are having the same experience.

Using Microsoft Operations Manager (MOM) 2005 as a monitoring tool allows you to identify potential problem areas in Active Directory before your users do. However, monitoring and managing directory services also requires

understanding what is occurring with the services AD requires (the base operating system and Domain Name System [DNS] services) and the services that require AD (Microsoft Windows File Replication Service [FRS] and Group Policy).

Using Management Packs to Manage Directory Services

This chapter discusses using MOM and its management packs to monitor the system resources, core network services, and high availability technologies at the heart of an Active Directory environment. Using MOM 2005 can give you a better understanding of your overall environment and help you quickly identify operational problems, preferably before users and applications are impacted.

An Active Directory environment includes configuration, schema, domain, and application partitions in addition to the well-known users, groups, and computers objects. Each domain controller (DC) contains a copy of its own domain partition, the configuration and schema partitions, and can host additional partitions. These partitions are replicated between domain controllers. Monitoring the health of the directory and replication consistency between domain controllers is essential in properly maintaining a Windows server domain environment.

No single management pack addresses all aspects of managing directory services. Microsoft and various third-party vendors provide a monitoring solution using a combination of management packs; the ones you implement will depend on your specific requirements.

Management Packs for Monitoring Active Directory

If you use the Active Directory Management Pack as suggested we also recommend you monitor the core operating systems with the Windows Server Base OS Management Pack, DNS using the DNS Management Pack, FRS using the File Replication Service Management Pack (which has a prerequisite of Ultrasound, discussed in the "Monitoring FRS" section later in this chapter), and finally Group Policy with the Group Policy Management Pack.

We discuss these management packs in the "Other Management Packs for Directory Services" section later in this chapter.

Active Directory Management Pack

The Active Directory Management Pack (ADMP) for MOM 2005 includes rules and scripts that monitor the health and availability of Active Directory components. The ADMP provides much of the monitoring functionality needed for Active Directory, and you should deploy it to all your Windows 2000 and Windows 2003 domain controllers. The ADMP provides you with easy access to key information such as

- Is replication occurring correctly?—Changes made on any domain controller replicate to all domain controllers sharing the relevant partition (domain, configuration,

schema, or application). Monitoring replication and ensuring replication consistency is one of the greatest challenges to Active Directory administrators. The ADMP monitors a wide variety of replication-related errors with out-of-the-box alerts to detect conditions indicating replication failures. The ADMP goes beyond simply watching for replication errors; it probes deeply into the health of connections between replication partners and monitors forestwide end-to-end replication.

- Is Active Directory authenticating users and responding effectively?—Active Directory authentication issues and response times are another challenge for Active Directory administrators. If Active Directory and/or Global Catalog response times are sluggish, user authentication becomes slow and email performance is negatively impacted.
- Are the Security Accounts Manager (SAM), NT LAN Manager (NTLM), Kerberos, and Local Security Authority Subsystem Service (LSASS) functioning properly?—Active Directory relies on these critical security components for authentication and authorization services.
- Is the Active Directory database inconsistent; does it have sufficient free space on its host volume?—Problems with the AD database can cause affected domain controllers to become nonfunctional.
- Are key dependency services such as DNS, FRS, W32Time (the Windows Time Service), and the System Volume share (SYSVOL) functioning correctly?—Problems with these services account for a high percentage of Active Directory failures; the ADMP includes basic monitoring of their functionality.

The ADMP also contains a client pack. We suggest deploying the client pack to servers hosting directory-enabled applications such as Exchange, giving you the capability to monitor AD response from the client application's point of view. We discuss client monitoring in the "Deploying the ADMP Client Pack" section later in this chapter. The client pack answers questions including the following:

- Are Lightweight Directory Access Protocol (LDAP) queries being resolved, and how quickly are they processed?—LDAP is the primary interface to Active Directory clients, and LDAP-based applications including Exchange depend on this protocol to access information from the directory. The ADMP tests LDAP functionality by performing LDAP binds and searches against domain controllers and monitors for LDAP-related events in the Directory Service logs.
- Are the Global Catalog servers functioning correctly?—The Global Catalog (GC) contains partial replicas of objects from all domains in the forest and is necessary in many scenarios (such as Microsoft Exchange email) for user logon and access to objects throughout the forest. The ADMP tests Global Catalog functionality in similar ways that it tests LDAP.

The ADMP provides forestwide monitoring and monitors trust relationships with domains both inside and outside the forest. The management pack is the primary tool used by Operations Manager for monitoring directory services and determining whether Microsoft

Windows directory services are working correctly. The ADMP is designed to provide status of your Active Directory environment with tools to quickly diagnose and resolve issues.

ADMP Functionality

When administrators think of monitoring Active Directory, they often think in terms of monitoring security-related changes, such as adding users to key administrative groups. The Active Directory management pack monitors the health and performance of the directory; it does not track changes to specific objects stored in it. The ADMP does not include audit functionality for monitoring changes to security sensitive objects or other key directory objects such as sites, subnets, and schema.

Third-party software such as Secure Vantage's System Controls Management Pack (SCMP), discussed in Chapter 15, "Managing the Operating System," monitors security changes to Active Directory. We provide the SecurityPack, discussed in Chapter 20, "Developing Management Packs," to monitor events in the Windows Security event log.

Status Views

The Operator console includes three topology views to help monitor Active Directory. These views provide status information for your Active Directory environment:

- Site Links (Site → Site), illustrated in Figure 16.1.

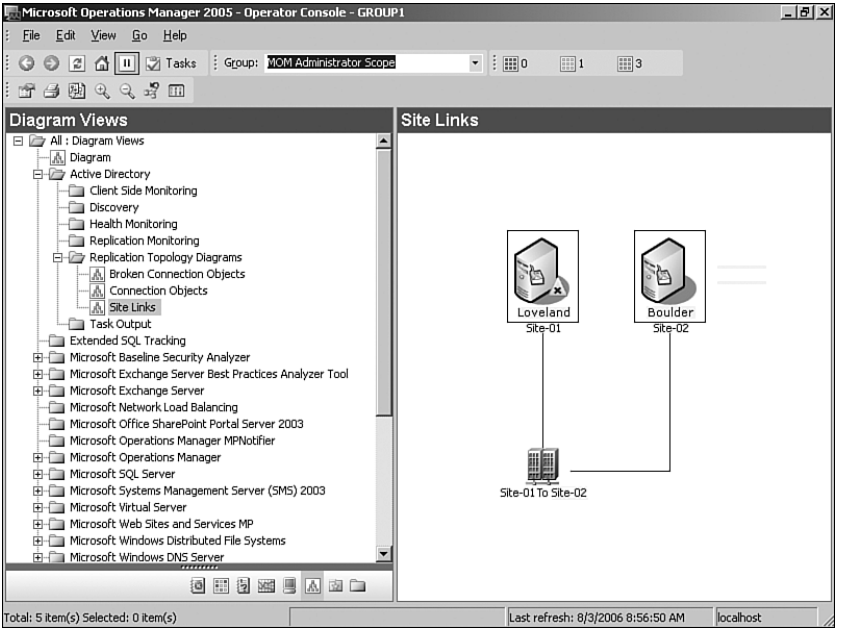


FIGURE 16.1 Site Links Active Directory topology view.

- Connection Objects (DC → DC), illustrated in Figure 16.2.

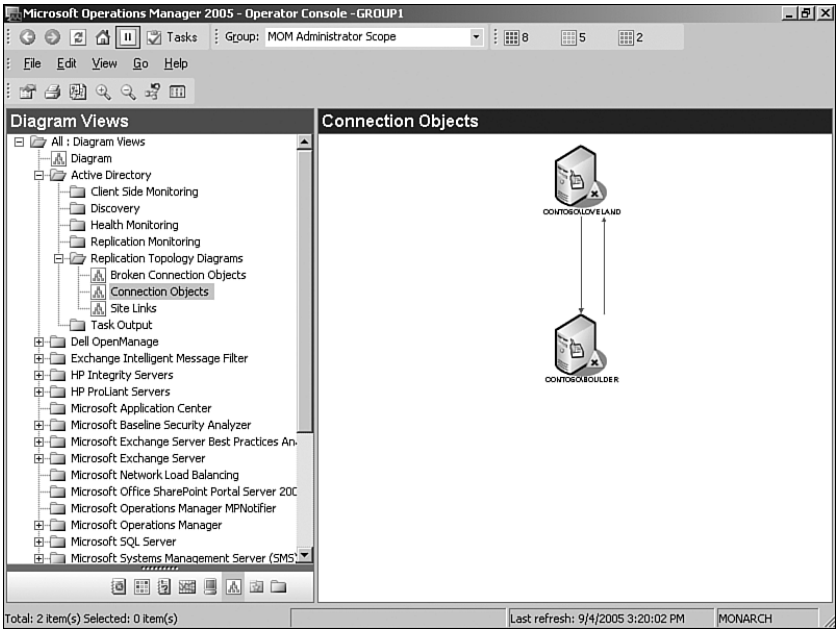


FIGURE 16.2 Connected Objects Active Directory topology view.

- Broken Connection Objects displays connection objects that exist between the domain controllers on your network that are in an error state, illustrated in Figure 16.3.

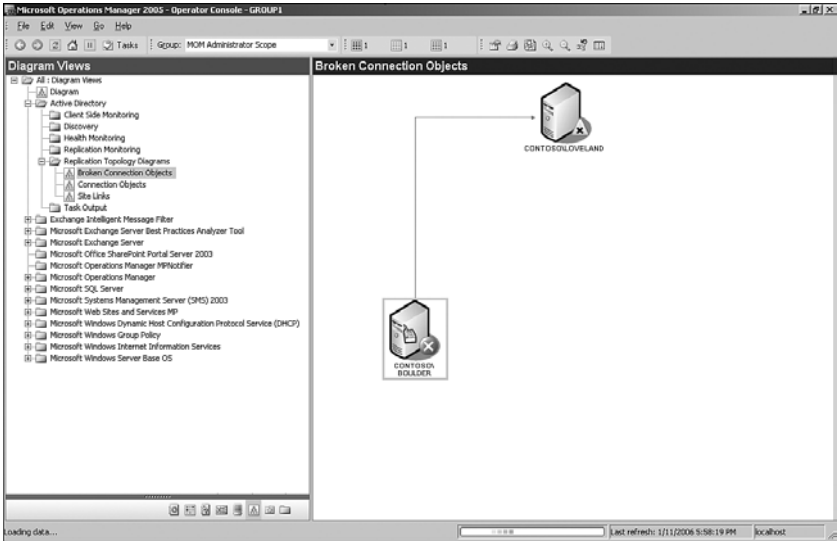


FIGURE 16.3 Broken Connection Objects Active Directory topology view.

Locate, Download, Install

Download the Active Directory Management Pack for MOM 2005 from the Management Pack Catalog at http://go.microsoft.com/fwlink/?linkid=43970 and follow the procedures documented in Chapter 13, "Administering Management Packs," to extract and install the management pack. Reports are included with the ADMP, so if you use MOM Reporting, choose the Import Management Packs and Reports option during the import process. If agents are not yet deployed to your Active Directory domain controllers, those servers need the MOM agent installed before MOM deploys the ADMP rules to those systems.

Active Directory Providers on Windows 2000

The ADMP uses two Windows Management Instrumentation (WMI) providers to gather data for the management pack. These are the ReplProv and TrustMon providers, which come with Windows Server 2003 but must be installed on Windows 2000 domain controllers for the ADMP to function. ReplProv provides access to Active Directory replication API calls through the WMI interface. TrustMon provides information about the trust relationships between domains. The ReplProv.msi installs the WMI classes required for both ReplProv and TrustMon and is available on the MOM 2005 installation media in the SupportTools directory.

In addition, if you are monitoring Windows 2000 DNS servers you should install the Windows 2000 DNS WMI provider on those servers. The provider is available in the Windows 2000 Server Resource Kit, or you can download it from ftp://ftp.microsoft.com/reskit/win2000/dnsprov.zip.

Microsoft provides management pack guides that include in-depth technical details and configuration steps for some management packs including how to deploy them. The Microsoft Active Directory Management Pack Guide can be downloaded from the website location for the management pack guides, http://go.microsoft.com/fwlink/?linkid=49776.

Real World—Deploying the ADMP

Ideally, you would deploy the ADMP at the beginning of your Active Directory deployment. In our not-so-perfect world, you will often implement the ADMP into an existing AD environment—so you need to take care not to overwhelm MOM (and your administrators) with a backlog of data about preexisting issues.

Using a phased approach, deploy the management pack to several domain controllers at a time rather than to your entire infrastructure. You might consider deploying the ADMP on a site-by-site basis, and deploying the client pack to one class of application servers at a time. With a gradual rollout, you have the chance to tune your monitoring strategies as you go along. You can achieve this by tightly controlling when the agent is deployed onto your domain controllers, and managing the membership of the computer groups that the ADMP uses.

Rules and Alerts

There are hundreds of performance and event rules within the ADMP, including rules testing the health and performance of domain controllers, verifying trusts, and monitoring time synchronization, Group Policy application, and Kerberos authentication. Some of the more important events to watch for include

- CPU is overloaded. If not corrected, high CPU utilization can seriously degrade domain controller performance. For information about troubleshooting high CPU usage on domain controllers, see the Active Directory Operations Guide: Troubleshooting High CPU Usage on a Domain Controller at http://go.microsoft.com/fwlink/?linkid=49837.
- The LSASS Process is using a high percentage of available CPU time. This is common on domain controllers and generally results from rapid authentication retries or inefficient LDAP queries. In both these cases, the most likely cause is a misbehaved application, but it may also indicate a network attack.
- A journal wrap error occurred in the SYSVOL. If the FRS is experiencing journal wrap errors on a server, file replication stops until the condition is cleared. For information on causes of journal wrap errors and troubleshooting these conditions, see Active Directory Operations Overview: Troubleshooting File Replication Service at http://go.microsoft.com/fwlink/?linkid=49836.
- FRS has not replicated one or more files in the SYSVOL to other domain controllers. This may be caused by excessive replication, often due to virus scanning or other processes opening files on SYSVOL.
- Multiple time synchronization errors are reported. Time synchronization is essential to Active Directory functioning including Kerberos authentication. You should investigate repeated errors from the W32Time service.
- The Active Directory database is corrupt. This indicates a serious problem and must be investigated immediately.
- Database excessive growth warning. Growth of the database or logs may be normal, for example, if new AD integrated DNS zones were added recently; however, you should investigate unexplained excessive growth.
- Database log file excessive growth warning. Active Directory uses circular logging in a file named edb.log. The edb.log is fixed at 10 megabytes (MB) in size and when it fills is renamed to edbxxxxxx.log and a new edb.log is created. The edbxxxxxx.log files are automatically deleted as transactions are written to the database. If multiple edbxxxxxx.log files are created but not deleted it may indicate a performance problem where the domain controller is not keeping up with the changes and transactions are not being committed.

Excessive Growth Warning Fix

Excessive growth also occurs from a bug that caused the log files to not clean up correctly in Windows 2000 domain controllers but was fixed with Windows 2000 Service Pack 2.

- Active Directory cannot update an object because the disk containing the database is full. This condition should be corrected immediately.
- Could not determine Flexible Single Master Operations (FSMO) role holder. The FSMO role holders are essential to proper functioning of Active Directory. A failure to determine the FSMO role holder often results from replication inconsistency. Additional rules that ping and bind to each of the FSMO role holders test the availability of these specialized servers.
- New account Security Identifier (SID) cannot be set. This may indicate a problem with the Relative Identifier (RID) master FSMO role.

Synthetic Performance Metrics

The ADMP does not simply rely on the built-in performance counters that Microsoft ships with Active Directory. The problem with these counters is that for the most part they are all server-centric, meaning that they measure values that are relevant to the server but may not reflect the end-user experience. This parochial view does not work if you are trying to measure the performance of a multiserver distributed service. To do that you need to get measurements that are service-centric and span multiple servers.

The ADMP uses scripts to synthetically generate these performance counters. We discuss many of these scripts throughout this chapter. The types of counters they generate include

- Active Directory response times to clients
- Operations masters response times to clients
- Global catalog search times from clients
- Replication latency
- Active Directory database size
- Active Directory log size

These synthetic counters are in addition to the standard performance counters exposed by Active Directory, such as the DRA inbound and outbound bytes counters, LDAP Client Sessions counter, and Kerberos Authentications counter within the NTDS object.

Configuring the Active Directory Management Pack

Before configuring the ADMP, planning is critical to ensure that the actions of the management pack do not negatively affect your infrastructure. The Roman physician Galen wrote in Latin in the second century AD *"Primum non nocere"*—"First, do no harm." Planning ensures that deploying the management pack follows this sage advice. For example, the synthetic transactions the ADMP introduces will place a real load on the systems, which means that the transactions should be carefully tested and deployed. There are a series of questions you can ask to put a framework around this. Some of the questions to ask in planning for the deployment of the Active Directory management pack are as follows:

- What are your Service Level Agreements (SLAs)?—Active Directory may or may not have specific SLAs in you organization, in which case you can always fall back to what the system was intended to accomplish. In the case of the Active Directory and the ADMP, critical SLAs are typically replication related.
- What impact will the management pack have?—This includes the impact on the domain controllers themselves and the network infrastructure such as Wide Area Network (WAN) links.

  Another aspect is the impact of the management pack on the management infrastructure, such as the database growth or alert generation. If you configure client-side monitoring, it is critical to identify the systems that need to participate in the client-side monitoring rather than configure all servers to participate. Either that or you need to ensure that the database can handle the additional load and storage requirements.
- What rights does the management pack need?—To execute its tasks, the ADMP needs certain minimum rights. The various scripts have different requirements that the standard deployment will provide. However, if you operate in a locked-down environment, you may need to specifically grant the rights to allow some of the scripts to operate.
- What needs to be installed on the agents, management servers, and for the operator consoles?—The ADMP requires some software to be preinstalled on the domain controllers and the management servers to operate properly, which is primarily to run tasks. The main requirements are to load the Support tools on the domain controllers and to load the Administrative Tools on the management servers.

Once you have the basic questions answered and have taken the actions dictated by the answers to those questions, you are ready to begin your installation. We recommend several configuration steps when deploying the Active Directory MP:

- Specify domain controllers for data collection to monitor replication latency.
- Modify the default value of the intersite replication latency threshold.

- Configure the ADMP to use a low privilege security account; however, this approach restricts what the ADMP can monitor.
- Minimize the impact of monitoring slow or saturated WAN links.

ADMP with Windows 2000 Domain Controllers

If you use MOM 2005 SP1 to monitor Windows 2000–based domain controllers, you may receive script error events indicating that the AD Global Catalog Search Response script cannot locate a global catalog. A hotfix is available from Microsoft to fix this issue at http://support.microsoft.com/kb/922338/. Install this hotfix on each Windows 2000 domain controller monitored by MOM.

Replication Monitoring

Replication consistency is essential to the health of the directory, and watching replication closely can alert you to many other problems in your environment. Successful replication depends on the proper functioning of network connectivity, DNS, Remote Procedure Call (RPC), LDAP, time synchronization, and Kerberos authentication services. Although you should monitor each of these services separately, replication success or failure is often a good indicator of the health of the services it depends on. Indicators of replication performance include intersite replication latency and replication latency data collection.

Replication Latency Data Collection For the AD Replication Latency report to provide data, you must specify both source and target domain controllers that will collect information:

- Specify the source domain controllers by opening the MOM Administrator console under Management Packs \ Computer Groups \ Active Directory Replication Latency Data Collection - Sources; then right-click and choose Properties. On the Included Computers tab, select the computers to add to this group.
- Use the same process for the target domain controllers by changing the computers included on the Active Directory Replication Latency Data Collection - Targets group.

After committing your changes, it may take up to 24 hours to begin collecting data.

MOMLatencyMonitors The ADMP creates an AD container named MOMLatency Monitors. This container is visible in the Active Directory Users and Computers console if you click on View and check the Advanced Features option.

The container is created by the AD Replication Monitoring script. If the script cannot create the container, you will receive an alert that "The script 'AD Replication monitoring' encountered a permissions error; the script failed to create the MOMLatencyMonitors container in the naming context 'DC=contoso,DC=com' because access was denied."

You can add the container manually by performing the following steps on a domain controller, preferably the DC providing the Primary Domain Controller (PDC) Emulator role:

1. Go to Start, click Run, and type **ADSIEdit.msc**.
2. Within ADSIEdit, double-click the Domain [*computername*], and then right-click DC=*domainname*,DC=com (for our environment the c*omputername* would be Monarch, and the DC= strings would be DC=contoso,DC=com).
3. Click New and then choose Object.
4. For the Select a class option, choose Container and then click Next.
5. For the Value, type **MOMLatencyMonitors** and then click Next.
6. Click Finish to complete adding the container.

You only need to create the container on one domain controller; it will replicate to the other domain controllers within the forest.

Intersite Replication Latency *Intersite replication latency* (the amount of time it takes for a change to a directory object to replicate throughout the forest) is a key indicator of replication performance. This is the maximum expected time that it takes for domain controllers to replicate across the entire Active Directory forest. If an object is created or changed at the farthest domain controller in the organization, the intersite replication latency is the maximum time it should take for the change to be seen on the domain controller at the other end of the organization. Typically, this will be between branch offices in a standard hub and spoke topology. Most organizations have no idea what the replication latency is at any given time.

The ADMP Script - AD Replication Monitoring rule monitors replication by creating a MOM event if the maximum replication latency exceeds a defined threshold. An alert is generated when a MOM event of classification Error or higher is created from the Active Directory Availability group.

This Script - AD Replication Monitoring rule is located in the Administrator console at Management Packs \ Rule Groups \ Microsoft Windows Active Directory \ Active Directory Windows 2000 and Windows Server 2003 \ Active Directory Availability \ Event Rules \ Script - AD Replication Monitoring. The default threshold is set at 15 minutes. For a small company with single-hop links, the default 15-minute setting is good. For a larger company with distributed multihop links or even a medium-sized company with a hub-and-spoke network, the value should be higher. The value should be set to a maximum time it should take for an object to replicate.

We suggest you determine this value during the AD design process; you can then align service-level agreements for services that depend on AD replication, such as password changes, with this value.

Information on AD Replication Topology

Resources to assist you in determining appropriate values are available in the Active Directory Replication Technologies section of the Windows Server 2003 Technical Reference, at http://go.microsoft.com/fwlink/?linkid=49778.

After determining an appropriate threshold, set the intersite replication latency threshold value using the following procedure:

1. In the MOM Administrator console, locate the Script - AD Replication Monitoring event rule under Management Packs \ Rule Groups \ Microsoft Windows Active Directory \ Active Directory Windows 2000 and Windows Server 2003 \ Active Directory Availability \ Event Rules.

Watch Where You Find the Script!

MOM has two major ways that you can locate scripts to change them. The first way is locating the rule that uses the script and make the modification from there (this is the recommended method). The second approach is to find the script under the Management Packs \ Scripts section. This is not suggested because it is easy to modify the wrong script.

2. Open the Properties for the rule and click on the Responses tab.
3. Double-click the AD Replication Monitoring script, and under Script Parameters, double-click IntersiteExpectedMaxLatency. See Figure 16.4 for an illustration. Enter the appropriate value and confirm all dialogs.
4. Commit the configuration changes.

Look Carefully!

The `IntrasiteExpectedMaxLatency` parameter is right below the `IntersiteExpectedMaxLatency` parameter and can be easily confused with `IntersiteExpectedMaxLatency`. While the Intersite parameter measures latency across the forest between sites, the Intrasite parameter measures latency within a given site. Based on the Active Directory architecture, this should always be less than 5 minutes.

Replication Latency Data Collection The ADMP collects data for replication performance over time using Replication Latency Data Collection. By default, the ADMP does not collect replication latency information, even though you specify Intersite Expected Maximum Latency and enable the rules. To avoid undue impact on the environment and on the management infrastructure, the ADMP by default does not have any domain controllers participating in the replication latency testing. To include domain controllers in the testing, you simply add them to the appropriate computer groups.

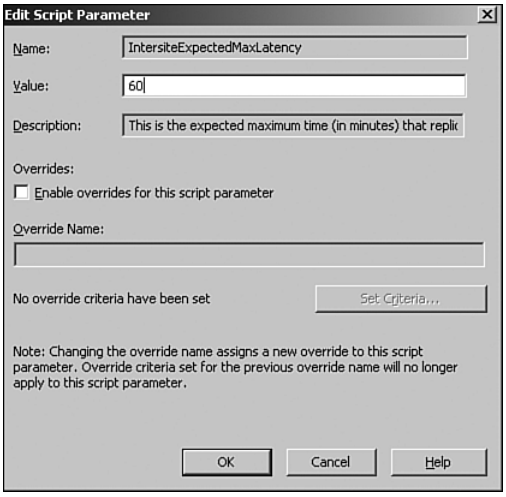


FIGURE 16.4 The Edit Script Parameter window.

There are both sources and targets for the replication testing with corresponding groups, which allows you to customize how you want the replication measured. The sources of replication (the domain controllers that create the objects) are specified in the Active Directory Replication Latency Data Collection - Sources computer group. The targets of replication (the domain controllers that check for the objects) are specified in the Active Directory Replication Latency Data Collection - Targets computer group.

The data is collected on source and target domain controllers you specify and can be used to view a graphical representation of historical trends in replication latency. Because a considerable amount of data is collected, you will want to limit the number of DCs used for data collection. Perform the following steps to specify the domain controllers for data collection:

1. In the Administrator console, locate Computer Groups \ Active Directory Replication Latency Data Collection - Sources and open the properties for this group.
2. Click on the Included Computers tab and select the appropriate domain controllers; then click OK. Note that you can also add computer groups on the Included Subgroups tab.
3. Perform the same task for the Active Directory Replication Latency Data Collection - Targets group.

Although we used the included computers function of the computer group, you could also use any of the other methods to determine group membership to populate the group. For example, if there is a formula that will work to determine membership of either of the groups, you could use that instead. The benefit is that the membership generates automatically without configuration.

Perhaps a company needs to monitor replication latency between all branch office domain controllers but does not want to include all domain controllers in the environment. To automatically add appropriate domain controllers to the replication latency, you need a formula including all domain controllers except those in the Site-02 site. To implement this, simply collect a SiteCode attribute (registry location HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\Site-Name) and configure the group memberships as shown in Figure 16.5. This will ensure that new domain controllers in branch offices will be included in the replication latency monitoring automatically.

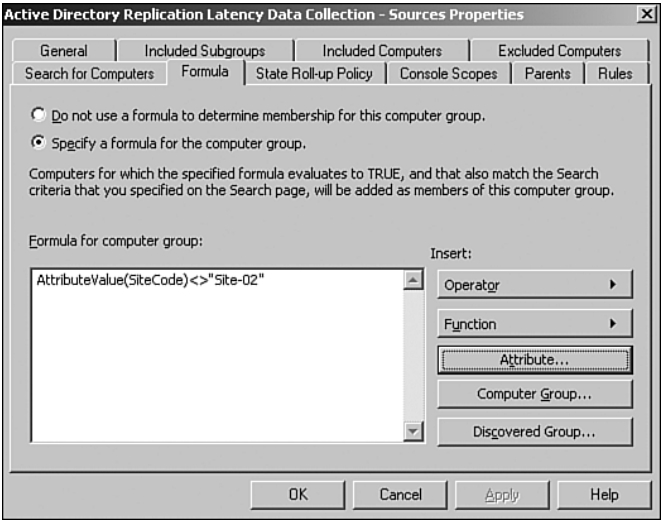


FIGURE 16.5 Computer group excluding Site-02.

After enabling the replication latency monitoring by placing domain controllers in the appropriate groups, it may take up to 24 hours for the first latency metrics to be generated.

Using a Minimum Privilege Action Account

Windows 2000 domain controllers using the ADMP require that the MOM Agent Action account be a member of the Domain Admins group in the forest root domain. In Windows Server 2003 highly secure installations, you may want to use a nonadministrator Action account. Several configuration steps are required to use a less privileged account:

- The Agent Action account must belong to the Users and the Performance Monitor Users local security groups and have access to the event logs.
- The account requires the Allow Log on Locally, Generate Security Audits, and Manage Auditing and Security Log user rights.

- Both the Action account and the MOM Service account must have full control access on the CN=MomLatencyMonitors container in Active Directory for each directory partition you monitor.

These two accounts also need read access to the registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\NTDS\Parameters and the file system directories containing NTDS.dit and the Active Directory log files (both by default located in the %*SystemRoot*%\ntds directory). In a low-privileged scenario, the ADMP requires that the account used for the Action account and the service context that the MOM service runs under have additional rights and privileges. Table 16.1 lists the access types that must be configured manually.

Windows 2000 Action Accounts

Windows 2000 servers cannot use a low privilege account; the Action account must be an account with at least local administrative privileges on the Windows 2000 server.

TABLE 16.1 Access Types Required by the Active Directory Management Pack

Resource	Access Type	Instructions
CN=MomLatencyMonitors Container	Full	The Action account must be able to: ▶ Create container objects as children of CN=MOMLatencyMonitors ▶ Read attributes of all objects created under CN=MOMLatencyMonitors ▶ Write to the adminDescription attribute on objects created under CN=MOMLatencyMonitors. ▶ Create the MomLatencyMonitors container as a child container of the root of each domain and application directory partition you are monitoring. If an application directory partition crosses domain boundaries, give appropriate access to the Action account in each domain. To monitor the configuration partition, create the MomLatencyMonitors container as a child object of the configuration partition using ADSIEdit.msc. The MomLatencyMonitors container needs to be created on only one domain controller because the created object replicates to other domains in the forest.

TABLE 16.1 Continued

Resource	Access Type	Instructions
Registry keys	Read	Add the Action account to the registry properties of HKLM\SYSTEM\CurrentControlSet\Service\NTDS\Parameters, providing Read access. Read access enables the Action account to find the location of NTDS.dit and the Active Directory log files. Add the Action account to the registry properties on each domain controller.
Directories containing NTDS.dit and Active Directory log files	Read	The Action account must have Read access to the file path location of NTDS.dit and the Active Directory log files. The directory location of NTDS.dit is the *%SystemRoot%*\ntds directory, and the Active Directory log files are also there by default. Provide access to the file path location on each domain controller.

The Action account must belong to either the Domain Admins group or the Administrators group in the domain where the AD Monitor Trust script monitors trusts. If the Action account is not a member of one of these groups, you receive a failure message on the script unless you disable the Script - AD Monitor Trusts rule. This rule is located in the MOM Administrator console, under Management Packs \ Rule Groups \ Microsoft Windows Active Directory \ Active Directory Monitor Trusts \ Event Rules. The alert sends a notification to the Network Administrators Notification group if a severity of at least "error" occurs from rules within the Active Directory Monitor Trusts rule subgroup.

Bandwidth Considerations

If your network has slow or unreliable WAN links or many branch offices, you may want to reduce the amount of traffic MOM generates when monitoring Active Directory by disabling the Active Directory reporting rules. Select each group, double-click on it, and clear the Enabled check box:

- Microsoft Windows Active Directory \ Active Directory Windows 2000 \ Reporting Rules for Active Directory
- Microsoft Windows Active Directory \ Active Directory Windows 2000 and Windows Server 2003 \ Reporting Rules for Active Directory
- Microsoft Windows Active Directory \ Windows Server 2003 \ Reporting Rules for Active Directory

Alternatively, you could configure overrides for each rule in these groups to exclude servers across slow links, as listed. This is shown in the following procedure:

1. Go to each rule in the groups listed in this section, open the Properties page, and select the General tab.

2. Check the Enable Rule-Disable Overrides for this rule and set the Override Name to a more intuitive name such as SlowLink_RuleDisable.
3. Click on Set Criteria and add each target computer or computer group using the default value of Disable (0).
4. Click OK on each page and then move on to the next rule within the group.

Deploying the ADMP Client Pack

The ADMP client pack enables you to simulate AD response for a client application. The client pack includes a rule group and a computer group. The event rules verify client directory access, and the computer group specifies which computers will run these rules.

The ADMP generates synthetic transactions from clients to test connectivity proactively, giving you a clear signal of how the domain controllers and Active Directory are responding from the client perspective. The client computers run tests to determine whether the domain controllers are available, using the following methods to each domain controller it is monitoring:

- Pings with Internet Control Message Protocol (ICMP)
- Pings with Lightweight Directory Access Protocol (LDAP)
- Establishing a Net Use Connection to the SYSVOL share
- Performing an LDAP bind
- Performing an LDAP search

Thresholds are specified and can be adjusted for the LDAP bind and search. If multiple consecutive failures (or binds or searches that exceed the specified thresholds) occur, an alert is generated. In addition, the client computer also determines whether:

- The client can contact a domain controller in its local site.
- A sufficient number of global catalog servers is available.

Each *client computer* (a computer that is not a domain controller running the MOM agent and this rule group) can be configured to monitor only the domain controllers of interest. You can configure the clients to

- Monitor a specific list of domain controllers.
- Monitor domain controllers in the client's local site.
- Monitor domain controllers in a list of specified sites.
- Monitor all domain controllers in the client's domain or in a specified list of domains.

The settings are configured on the Script - AD Client Update DCs rule in the Active Directory Client Side Monitoring rule group.

You should configure both the rule group and the computer group. The client pack requires the MOM agent. It is not designed to scale to client computers such as laptops and desktops in a large deployment. To deploy the ADMP client pack to the appropriate machines perform the following steps:

1. In the MOM Administrator console, open the properties of the Active Directory Client Side Monitoring computer group.
2. From the Included Computers tab click Add and select individual computers to which you want to deploy the client pack. From the Included Subgroups tab, you can add computer groups as shown in Figure 16.6.

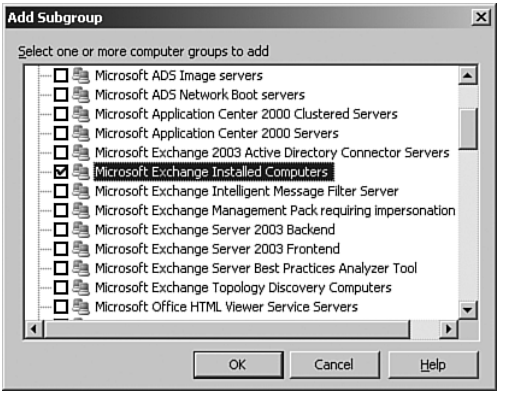


FIGURE 16.6 Adding subgroups to deploy the client pack.

Deploying the Client Pack

If administrative boundaries or business considerations preclude deploying the client pack to an application server, you should deploy it to a machine that is close to that server in the network topology.

The client pack can be installed on any system running the MOM agent; however, we recommend installing it on a member server rather than a domain controller because the intent of the client pack is to provide a client's perspective on Active Directory.

Computers using the client pack must have their agent proxy settings modified. This is done with the following steps:

1. In the MOM Administrator console, navigate to Computers \ Agent Managed Computers.

2. Right-click on the domain controller (the one that the client pack is monitoring) that you want to configure agent proxying settings and then click on Properties.
3. On the Security tab, clear the Use Global Settings check box and then clear the Prevent Agent from Proxying for Other Computers or Network Devices check box.

Client-side monitoring tests basic connectivity using ICMP and LDAP ping. It also tests connectivity to the SYSVOL share. Client-side rules verify connectivity and test availability to domain controller roles including the PDC emulator, local domain controllers, and global catalog servers. Scripts are included to execute LDAP binds and searches.

Client-side monitoring rules are located in the Active Directory Client Side Monitoring rule group. You can configure the parameters in this rule group based on requirements of your particular applications. As an example, the minimum number of available GCs contactable by the client is set to 3 by default. This can be changed using the MOM Administrator console under Management Packs \ Rule Groups \ Microsoft Windows Active Directory \ Active Directory Client Side Monitoring \ Event Rules by changing the script parameter value for MinimumAvailableGCs as part of the Script - AD Client GC Availability rule.

Table 16.2 shows the parameters the script accepts.

TABLE 16.2 AD Client Connectivity Script Parameters

Parameter	Default	Range	Description
`BindThreshold`	500	1–60000	The number of milliseconds that a bind is allowed to take
`SearchThreshold`	500	1–60000	The number of seconds a search is allowed to take
`FailureThreshold`	3	1+	The number of consecutive failures allowed before an alert is generated
`LogSuccessEvent`	False	True or False	Specifies whether the script should log success events

There is a hard-coded constant `MAX_REPEAT_COUNT` within the script that is used by the ping test to set the maximum number of times it will retry the test. It is set to 2 by default but can be adjusted in the script. The script includes logic to set the `FailureThreshold` to 3 if the parameter is set to less than 1. The script also includes logic to adjust the thresholds if they are set higher than 60,000 milliseconds, in which case the script forces the `BindThreshold` to 1000 and the `SearchThreshold` to 2000.

The script parameters can be set by passing in global parameters from the rule or by manually editing registry settings on each agent as shown in Table 16.3.

TABLE 16.3 Manual Setting of Client-Side Monitoring Tests

Purpose	Registry Key	Registry Values	Example Value
Test	HKLM\SOFTWARE\Microsoft\Microsoft Operations Management\AD Management Pack\Tests	`BindThreshold`	500
Test	HKLM\SOFTWARE\Microsoft\Microsoft Operations Management\AD Management Pack\Tests	`SearchThreshold`	500
Test	HKLM\SOFTWARE\Microsoft\Microsoft Operations Management\AD Management Pack\Tests	`FailureThreshold`	3
Test	HKLM\SOFTWARE\Microsoft\Microsoft Operations Management\AD Management Pack\Tests	`LDAPPingTimeout`	10
Test	HKLM\SOFTWARE\Microsoft\Microsoft Operations Management\AD Management Pack\Tests	`LogSuccessEvent`	True

You might have noticed an additional manual parameter, `LDAPPingTimeout`, which cannot be set by the script parameters. The only way to set this value is in the registry. The maximum setting for this test parameter is 60, which the script checks and sets to the default of 10 if the registry setting is invalid.

Exchange Servers and Active Directory Client-Side Monitoring

Exchange services require access to domain controllers and specifically to the global catalog to function properly. You should always enable client-side monitoring of servers within the same Active Directory site, preferably on the Exchange servers themselves, to ensure that the Active Directory services are truly available from the Exchange server perspective.

If individual configurations are required for client tests, you can specify them through the registry on the agent-managed computer. You can overwrite any parameters specified at the MOM Administrator console by writing specified values in the registry on individual client computers. You can also use the registry to specify on a per-client basis the tests that will run and the parameters for those tests.

Client-Side Monitoring Domain Controller Discovery Setting

The script AD Client Update DCs runs once a day by default, shortly after midnight. The frequency is set through the Script - AD Client Update DCs rule. The script discovers the domain controllers for a client computer to run the client-side monitoring tests against.

The primary setting in this script is the `SiteDiscoveryMode` parameter. This parameter determines how the clients select domain controllers to test. The main configuration choices are

- Monitor all domain controllers in the domain—This is a relatively common setting for a small organization with a single domain. The `SiteDiscoveryMode` is set to 1 to enable this mode.

- Monitor all domain controllers in the site (default)—This is the default setting and is a good option for all organization sizes. It scales well because clients only test their local domain controllers. The `SiteDiscoveryMode` is set to 3 to enable this mode.
- Monitor all domain controllers in the forest—This is a relatively uncommon setting to choose because it has the potential to generate a lot of traffic. However, in some cases it might be necessary or used in some of the fine-tuning of the configuration. The `SiteDiscoveryMode` is set to 4 to enable this mode.

To set the Client Side Monitoring Domain Controller Discovery Setting in the management pack, follow these steps:

1. Launch the Administrator console.
2. Navigate to Management Packs \ Rule Groups \ Microsoft Windows Active Directory \ Active Directory Client Side Monitoring \ Event Rules.
3. Open the properties of the Script - AD Client Update DCs rule.
4. Select the Responses tab.
5. Select the AD Client Update DCs script and click the Edit button.
6. Select the `SiteDiscoveryMode` parameter.
7. Click the Edit Parameter button to edit the parameter.
8. Adjust the Value to the desired mode (the default is 3).
9. Click OK twice and then click OK again to save the change.
10. Commit the configuration changes.

On the next run, by default just after midnight, the client-side monitoring agents will update their list of domain controllers.

Tasks

The ADMP adds a number of tasks, giving you a single interface to identify and resolve issues within your Active Directory environment:

- Active Directory Users and Computer Snap-in—This snap-in is the main interface to configure users, groups, and computers within your Active Directory environment.

ADMP Task Prerequisites

For these tasks to function properly, you will need the Windows Administration Tools Pack (adminpak.msi), which includes the Active Directory Users and Computers MMC Snap-in. See Microsoft's knowledge base article 314978 at http://support.microsoft.com/kb/314978/ for information on installing the Windows Server administration tools.

You can download the most current version of the adminpak from Microsoft's download site, www.microsoft.com/downloads. Search for "adminpak."

- Active Directory Service Interfaces (ADSI) Edit—Used to view, modify, and set security on Active Directory objects.
- DCDIAG—Analyzes the state of the domain controllers and reports problems to assist with troubleshooting Active Directory issues. The DCDIAG task runs the Task Wizard and allows you to provide configurations for the ApplicationName, CommandInitialDirectory and the Parameters used for the DCDIAG application. The task does not provide a default parameter configuration, so you are required to provide the command-line parameters for it to function correctly. As an example, for our Loveland domain controller we configured the parameters field to be `/s:Loveland`.
- Enumerate Trusts—Lists the trust relationships between Active Directory domains. This task uses the Task Wizard and has parameters for CSV/Comma-Separated-Value format (defaults to False, which is tab delimited) and domains, defaulting to * for all domains.
- LDP—Performs LDAP searches against Active Directory by running LDP.exe without the Task Wizard to provide parameters.
- NETDIAG—Performs diagnostics to identify networking and connectivity issues. Similar to DCDIAG, NETDIAG starts the Task Wizard, and you can configure the command including the parameters to pass to NETDIAG. For example, for the Contoso domain the parameters would be `/d:contoso.com`.
- NETDOM—Maintains trust relationships and runs the Task Wizard to provide parameters to the application. Using the parameters for the task enables you to perform a variety of different trust-related functions. For example, if we wanted to verify the trust of the Fabrikam domain the syntax would be `netdom trust /d:Contoso Fabrikam /verify`.
- NLTEST—Displays the current list of trusted domains using the Task Wizard to provide parameters to the application. For example, to list the trusted domains we would set the parameter to `/trusted_domains`.
- REPADMIN—Assists in diagnosing replication issues between Active Directory domain controllers using the Task Wizard to provide parameters to the application. One example would be running a consistency check where we can set the parameter to `/kcc`.
- Replication Summary Snapshot—Runs the `repadmin /replsum` command to gather current replication status from a server. This task uses the Task Wizard to provide parameters for the application. This task defaults the parameters to `/replsum * /bysrc /bydest /sort:delta`.

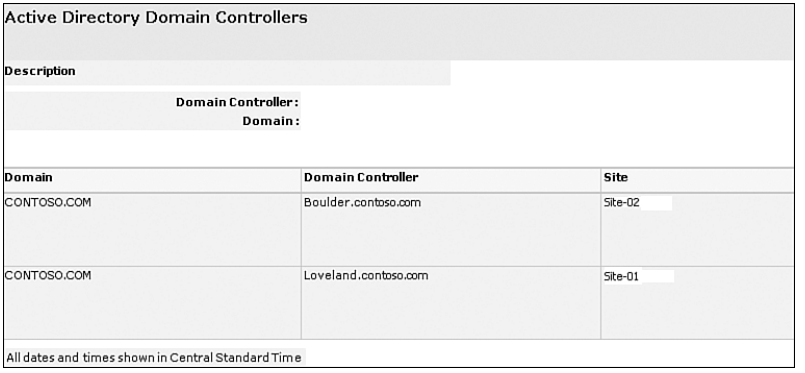
- Service Principal Name Health—Confirms Service Principal Names (SPN) health to diagnose replication authentication errors caused by bad SPN registrations. This task runs DCDIAG using the Task Wizard to provide parameters to the application. The default parameters are to `/test:MachineAccount /v`
- SETSPN—Manages Service Principal Names that are used to locate a principal name for running a service. This task uses the Task Wizard to provide parameters for the application. This task can be used to add or delete SPNs or to reset or list them depending on the parameters configured within the Task Wizard.

Reporting

If you need to look at the Active Directory performance information on a historical or long-term basis, reports are a good option. The report data is the same data that is in the operations database but is kept in this archive for a year by default.

The Active Directory folder contains multiple reports to assist monitoring your directory services environment including

- ADMP AD Replication Connection Objects—The report summarizes the AD replication topology. It provides a list of connection objects and indicates the source and target domain controllers and their respective sites, transport types, and whether the connection objects were manually configured.
- ADMP AD Replication Latency report—By summarizing minimum, average, and maximum replication latency, you can use the contents of this report to verify any Service Level Agreement (SLA) you have for changes replicating within a domain or forest.
- ADMP AD Replication Site Links—Shows the current replication site link configuration for Active Directory.
- ADMP AD DC Replication Bandwidth—Summarizes compressed and uncompressed replication bandwidth during a specified period. This report can be used for trending and capacity planning for replication bandwidth requirements.
- ADMP AD Domain Changes—This report summarizes significant changes to the domain, including moving the PDC emulator FSMO role and adding or removing domain controllers.
- ADMP AD Domain Controllers—This report, shown in Figure 16.7, lists all domain controllers in the specified domains, along with their Internet Protocol (IP) addresses and sites.
- ADMP AD Machine Account Authentication Failures—This report summarizes which machines joined to the domain are unable to authenticate. Authentication failures can prevent Group Policy updates and software distribution to the targeted system.
- ADMP AD Role Holders—Shown in Figure 16.8, these report computers holding one or more operations master roles or that are global catalog servers.



Active Directory Domain Controllers

Description

Domain Controller:
Domain:

Domain	Domain Controller	Site
CONTOSO.COM	Boulder.contoso.com	Site-02
CONTOSO.COM	Loveland.contoso.com	Site-01

All dates and times shown in Central Standard Time

FIGURE 16.7 AD Domain Controllers report.

Active Directory Role Holders Report

Microsoft Operations Manager 2005

Description

6/26/2005 1:23:08 PM

Name : <All>
Site : <All>
Scope Name : <All>

Role	Scope	Scope Name	Server	Site
Domain Naming Master	Forest Wide	contoso.com	Loveland.contoso.com	Site-01
Infrastructure Master	Domain Wide	DomainDnsZones.contoso.com	Boulder.contoso.com	Site-02
Infrastructure Master	Domain Wide	ForestDnsZones.contoso.com	Boulder.contoso.com	Site-02
Infrastructure Master	Domain Wide	contoso.com	Loveland.contoso.com	Site-01
PDC	Domain Wide	DomainDnsZones.contoso.com	Loveland.contoso.com	Site-01
PDC	Domain Wide	ForestDnsZones.contoso.com	Loveland.contoso.com	Site-01
RID Master	Domain Wide	DomainDnsZones.contoso.com	Loveland.contoso.com	Site-01
RID Master	Domain Wide	ForestDnsZones.contoso.com	Loveland.contoso.com	Site-01
Schema Master	Forest Wide	contoso.com	Loveland.contoso.com	Site-01

All dates and times shown in Central Standard Time

Page 1/1

FIGURE 16.8 AD Role Holders report.

- ADMP AD SAM Account Errors—The report summarizes events that indicate that the SAM has detected an error and provides corrective guidance where applicable.
- ADMP AD DC Disk Space—It is critical that Active Directory has adequate free space. This report, shown in Figure 16.9, summarizes AD disk space usage and free space for the database and log volumes. You can use this report to trend and predict the size of volumes you will need, given the current growth rate.

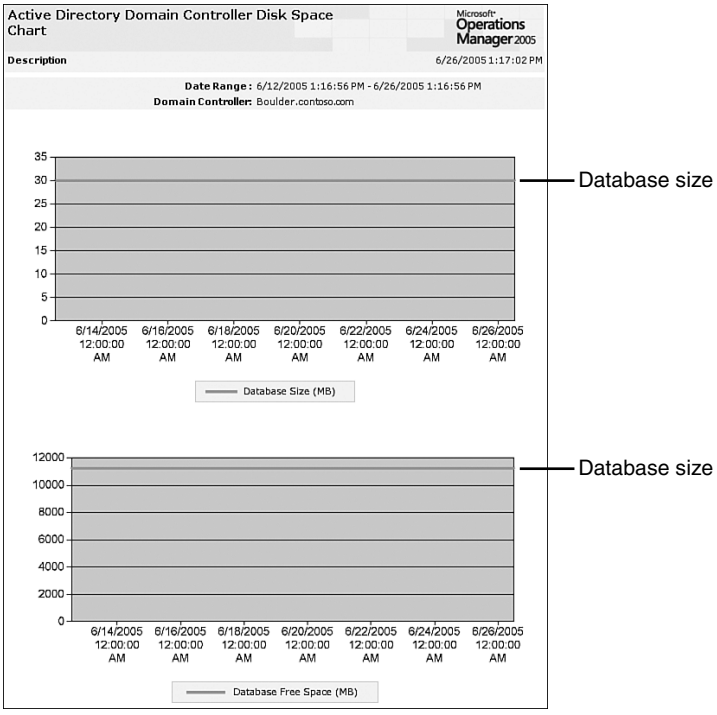


FIGURE 16.9 AD DC Disk Space report.

Other Management Packs for Directory Services

Building a solid structure requires a firm foundation. If you consider Active Directory as a house, its foundation includes the underlying operating system, DNS, and FRS. Each of these provides a piece required for a stable Active Directory architecture.

Monitoring the Underlying Operating System

A healthy AD environment needs a stable operating system running its domain controllers. You can use the Server Base Operating System Management Pack to monitor the operating systems on your Active Directory servers.

The Microsoft Windows Server Base Operating System Management Pack for Windows NT 4.0, Windows 2000, and Windows Server 2003 provides capabilities for monitoring server resources and services. Although Active Directory requires Windows 2000 and Server 2003, NT 4.0 servers may still use the Windows Base OS management pack for non–Active Directory domain controllers that have trusts with your Active Directory domains. You may also have NT 4.0 domain controllers in your domain if you are running Windows

2000 in AD mixed mode. NT 4.0 domain controllers must be monitored using the agentless method or with a third-party supplemental management pack. The Windows Server Base Operating System MP provides a comprehensive view of vital operating system components including

- System, application, and service availability—Availability of the system, applications, and services can be critical on domain controllers.
- Storage utilization—Running out of space on domain controllers can cause Active Directory to fail on the system.

If the operating systems of your domain controllers are not stable, directory services will not be stable. The Windows Server Base Operating System Management Pack provides useful information about Windows Server from NT 4.0 and up, although some functionality is specific to Windows 2000 and 2003. It answers questions such as the following:

- Are critical services running?—A service down can mean users are unable to connect to the domain controller. For example, domain controllers depend on the Netlogon service.
- Have services or applications terminated unexpectedly?—When services or applications terminate unexpectedly, outages can occur, and data can be lost.
- Has the server itself crashed, and what was the stop error?—When a server has crashed, having the stop code immediately available for online searches by product support professionals starts your troubleshooting process.
- Is the file system in good health with plenty of free space?—Low disk space or file system errors need to be addressed before the problem becomes critical.
- Are network errors occurring?—Servers depend on reliable network connectivity to service user requests and to access other servers such as domain controllers and replication partners.

Additional information for using the Windows Server Base Operating system Management Pack was provided in Chapter 15, "Managing the Operating System."

Rules

Several of the most critical operating system stability event rules are located in the Management Packs \ Microsoft Windows Servers Base Operating System \ <*Windows version*> \ reliability rule group. These include

- The Computer has rebooted from a bug check (collection)—Any automatic server reboot should be investigated because it can indicate serious conditions such as a hardware problem, failing or mismatched drivers, or a denial of service attack.

Using Bug Check Data

The bug check data collected by this rule is a great starting point for your investigation. Often the bug check parameters turn up exact causes in a search of the knowledge base, or will lead Microsoft Product Support professionals to a quick resolution.

- An application is repeatedly generating application errors—This rule indicates that an application has failed repeatedly (the default threshold is 4 failures) with "DrWatson" events, which indicate program or application errors. Repeated failures of this type indicate a serious problem with the application and should be investigated.

  Computer reboots and application errors directly impact the functionality of your domain controllers. Assign these issues a high priority and investigate them as quickly as possible.

Other Event Rules to Monitor

Look for other significant event rules located at Management Packs \ Microsoft Windows Servers Base Operating System \ <*Windows version*> \ Core System Components and Service group.

Drivers and services supply some of the core functionality required for Windows. Drivers provide an interface to computer hardware. Services are special types of applications that run in the background on a computer and can have permissions that regular applications do not. Drivers and services are monitored by rules within the Server Base Operating System management pack. The primary rule that checks for availability is the "The service or driver failed to start" rule. A failure in this category may represent a serious problem with the server.

Alerts

The Microsoft Windows Servers Base Operating System Management Pack provides an alert rule Send email or a page response for Alerts with severity of "Service Unavailable." This alert is included for the Windows 2000 and 2003 versions of the Windows Server operating system, and it can be configured from several nodes of the tree control in the Administrator console including Alert Rules under Management Packs \ Microsoft Windows Servers Base Operating System \ <*Windows version*> \ Reliability.

Many event and performance rules in the Core System Components and Service, Reliability and State Monitoring and Service Discovery rule groups have a severity level you can configure by using the Alert tab of their property sheets. If you configure this alert to send notifications, you can be automatically notified of events you set to a Service Unavailable severity. Further detail on alerts is provided in Chapter 14, "Monitoring with MOM."

Tasks

A number of tasks are included with the Windows Server Base Operating System MP. These tasks provide additional information and can diagnose potential issues for the servers MOM is managing. The list of tasks directly relevant to domain controllers are broken down into three major sections: local user information, routing information, and network information.

Local user information for the system is available via two queries:

- Local Users Query—Provides a list of local users on the specified server from servers including DCs
- User Account Settings Query—Provides a report of the current users on the server specified including password requirements and the server role

Three different tasks exist for debugging connectivity to and from domain controllers:

- Pathping—Runs a `pathping` from the MOM server to the specified server
- Route Print—Runs the `route` command with the `/print` option on the specified server
- Trace Route—Runs a `tracert` to the specified server

Network-based tasks gather information related to the connections currently made to the domain controller:

- NetStat - Display Total Active TCP Connections—Reports a count of total Transmission Control Protocol (TCP) connections by running the Netstat utility on the specified server.
- Network Statistics - Display Active Routes—Provides a list of active routes by running NetStat on the specified server.
- Network Statistics - Displays Active Connections—Reports a list of active connections gathered by the NetStat tool on the specified server. The `NetStat` command shows the connections, the port, and the state of the connections to the system (established, time_wait, close_wait). When used on a remote system this shows what specific domain controllers and ports are being used by the client.
- Network Statistics - Service Service Query—(This probably should be "Server Service Query," but this really is what the task is named!) Reports a list of network statistics for the Server service of the specified server.

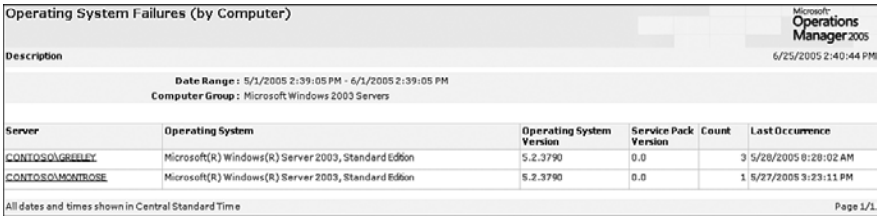
Reports

The reliability subgroup of the Microsoft Windows Servers Base Operating Systems reports contains reports on application and system failures, including the Operating Systems Failures (by Computer) report shown in Figure 16.10. Application crashes are reported on a per-server, per-event, or per-application basis; system crashes are reported per server, per

event or per stop code. If the reports provided with the management pack are not sufficient, you can create your own reports with specific information for your company's requirements.

Creating Reports

Chapter 21, "Using and Developing Reports," discusses the process of creating your own reports.



Operating System Failures (by Computer)

Microsoft Operations Manager 2005

Description

6/25/2005 2:40:44 PM

Date Range : 5/1/2005 2:39:05 PM - 6/1/2005 2:39:05 PM
Computer Group : Microsoft Windows 2003 Servers

Server	Operating System	Operating System Version	Service Pack Version	Count	Last Occurrence
CONTOSO\GREELEY	Microsoft(R) Windows(R) Server 2003, Standard Edition	5.2.3790	0.0	3	5/28/2005 8:28:02 AM
CONTOSO\MONTROSE	Microsoft(R) Windows(R) Server 2003, Standard Edition	5.2.3790	0.0	1	5/27/2005 3:23:11 PM

All dates and times shown in Central Standard Time

Page 1/1

FIGURE 16.10 Operating Systems Failures (by Computer) report.

Monitoring DNS

Active Directory depends on a functioning DNS within your environment. Without a reliable DNS architecture you cannot have a stable Active Directory architecture. Active Directory uses DNS to locate domain controllers on the network, and Active Directory stores Service Location (SRV) and Address (A) records for the domain controllers within DNS. Active Directory cannot function without these records.

DNS is the standard name resolution method used to locate resources on the Internet and on most TCP/IP networks. DNS is also used in an Active Directory environment to define the AD namespace and locate essential services such as domain controllers. Microsoft DNS can integrate with Active Directory to take advantage of AD multimaster replication and security, although AD integration is not required.

Using Microsoft DNS

You are not required to use Microsoft's DNS for Active Directory although that is a typical configuration. To support Active Directory, DNS must support service records and should preferably support Dynamic DNS updates.

The DNS management pack can monitor the availability and performance of Microsoft DNS servers in your environment. It monitors whether DNS services are running and the health of the DNS database, registry configuration, backup, and replication. Additionally, the management pack detects runtime errors and events and measures response time for DNS queries. The DNS management pack provides answers to questions such as the following:

- Have problems occurred during the boot, initialize, and database load operations?
- Has corruption been detected in the DNS database or the DNS service registry records?
- Are zones properly configured and are zone transfers occurring successfully?
- Are the DNS servers responding to client requests such as recursive queries and dynamic registrations?

The DNS management pack helps you to manage your directory services through managing and monitoring one of the core dependencies of Active Directory.

Locate, Download, Install

Download the DNS management pack. The extract includes two significant files:

- MicrosoftWindowsDNS.akm - the management pack for DNS
- MicrosoftWindowsDNSReports.XML - report definitions

You can also download the Microsoft Windows DNS Server Management Pack Guide.

Rules and Alerts

The DNS Server management pack contains event rules related to boot failures, file failures, zone transfer failures, and so on. There are also performance rules associated with such DNS operations as query processing, updates, and caching. These rules are enabled by default. Depending on your environment, you may not need certain rules such as those related to Windows Internet Naming Service (WINS) integration. Disable any unnecessary rules. Unnecessary rules are those that do not assist in addressing issues.

The management pack collects service discovery data every 30 minutes by default. This number can be changed depending on your requirements. Changing the timing so that the script runs less frequently reduces the amount of overhead but also lowers the frequency of checking for connectivity. Reducing the value adds to the amount of overhead because the script runs more often, but you will find out sooner if there is a problem. The value can be configured in the DNS Service Discovery rule, located under Microsoft Windows DNS Server \ <*Windows version*> \ State Monitoring and Service Discovery \ Event Rules. Open the rule, and on the Data Provider tab select the DNS provider from the Provider Name list control and click Modify. Enter the desired value in the box for Generate Event Every _Minutes and confirm your selections.

Collecting DNS Service Discovery Data

Because Microsoft Windows DNS Server management pack collects service discovery data every 30 minutes by default, DNS-specific attributes might not appear in the MOM Operator console for up to 30 minutes after the management pack is deployed.

Configuring the DNS Management Pack

The DNS management pack includes an alert rule that sends notifications for all events with a Service Down severity. To take advantage of these alerts, populate the Network Administrators Notification Group with the appropriate operators responsible for DNS. You will also want to review the rules and disable any that are not relevant to your environment.

In highly secure installations, you may want to use nonadministrative credentials for the Agent Action account on Windows Server 2003. This requires several configuration steps:

- The Action account must be a member of the Users and Performance Monitor Users local groups and have access to the event logs. This account must also have Allow log on locally and Manage auditing and security log user rights.
- Both the Action account and the MOM Service account must have read permission to the DNS Server Zone information, which requires read rights to the WMI\root\MicrosoftDNS. These rights can be set within Active Directory Users and Computers on the Advanced view (or using the ADSIEdit utility) and must have the right to clear DNS cache and initiate DNS scavenging.

Windows 2000 Action Accounts

Remember that Windows 2000 servers cannot use a low-privilege account; the Action account must be a member of the local Administrators group.

Tasks

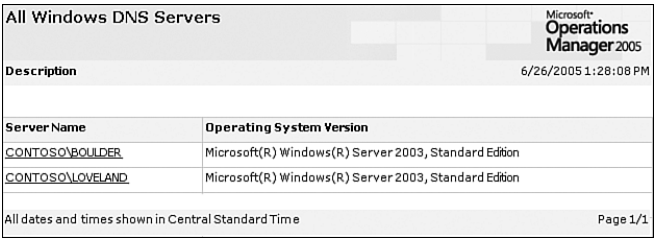
The DNS management pack includes a number of tasks, several of which you can use to diagnose and resolve DNS issues for your domain controllers:

- Clear DNS Cache—Clears out the DNS cache to remove stale DNS information.
- Start DNS Scavenging—Scavenges for orphaned or old records in DNS.
- Enumerate DNS Servers on a Windows 2003 Server—Provides information about the DNS server.
- Ping DNS Servers on a Windows 2003 Server—Sends a `ping` to the DNS servers to validate basic connectivity.

Reports

The Microsoft Windows DNS Server Report group provides extensive reporting capabilities including

- All Windows DNS Servers, illustrated in Figure 16.11
- All Windows DNS Zones by Server, illustrated in Figure 16.12



All Windows DNS Servers

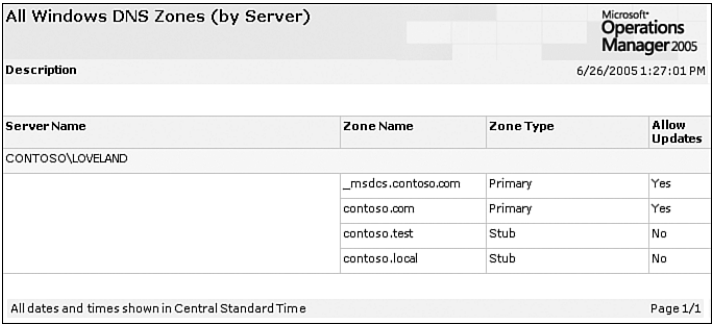
Microsoft Operations Manager 2005

Description 6/26/2005 1:28:08 PM

Server Name	Operating System Version
CONTOSO\BOULDER	Microsoft(R) Windows(R) Server 2003, Standard Edition
CONTOSO\LOVELAND	Microsoft(R) Windows(R) Server 2003, Standard Edition

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

FIGURE 16.11 All Windows DNS Servers.



All Windows DNS Zones (by Server)

Microsoft Operations Manager 2005

Description 6/26/2005 1:27:01 PM

Server Name	Zone Name	Zone Type	Allow Updates
CONTOSO\LOVELAND			
	_msdcs.contoso.com	Primary	Yes
	contoso.com	Primary	Yes
	contoso.test	Stub	No
	contoso.local	Stub	No

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

FIGURE 16.12 All Windows DNS Zones by Server.

Real World—DNS and AD Implementations

During initial deployments of Active Directory with Windows 2000, a well-known statement was that issues in Active Directory had a 90% likelihood of actually being within DNS.

Monitoring FRS

The Windows File Replication Service (FRS) is used to replicate files and folders in the SYSVOL file shares. SYSVOL contains Group Policy templates and login scripts that Active Directory uses. If the SYSVOL is not consistent, Group Policy errors and other issues can occur in your environment. FRS uses multimaster replication, meaning changes can be made at any location and will replicate to the other replica members. If FRS is not replicating information correctly, multiple issues can arise in your environment including inconsistent Group Policy application.

Windows 2003 R2 and DFS-R

SYSVOL replication changes with Windows 2003 R2, where Microsoft replaces FRS with Distributed File System Replication (DFS-R). In Windows 2003 R2 and later versions of Windows Server the FRS management pack is no longer required.

You can use the DFS Replication Service Management Pack to monitor the DFS Replication service running on Windows Server 2003 R2 DFS Folder targets. This management pack can be downloaded from the Management Pack Catalog website.

Locate, Download, Install

If you are using an earlier version of Windows Server than Windows Server 2003 R2, download the Windows File Replication Service (FRS) 2000, 2003 management pack for MOM 2005 from the Management Pack Catalog. The management pack guide for the FRS Management Pack is the File Replication Service MP Guide.

Rules and Alerts

The Windows File Replication Service Management Pack rules include items such as

- Replicas are in Critical or Warning State—Replicas are a copy of the data, which in the case of Active Directory is the SYSVOL contents. SYSVOL contains Group Policy information; if it is not correctly synchronized group policies will not apply consistently.
- Members are in Critical or Warning State—The server hosting the replica is in a member, and there are FRS problems on the server.
- FRS Connections are in a Critical or Warning State—The FRS connections between members have problems.
- Monitoring for Issues with Ultrasound—Discussed in the following section.

Configuring the Windows File Replication Service Management Pack

Installing the FRS management pack is straightforward, but the actual process to configure it may be more difficult depending on your environment. The FRS management pack is dependent on *Ultrasound*, a monitoring and troubleshooting tool for FRS available from Microsoft. There are also settings you can configure depending on your environment's specific requirements.

Ultrasound is available for download at the Microsoft download site, www.microsoft.com/downloads, by searching for "Ultrasound." Ultrasound is built of two major components: the Ultrasound Controller and the Ultrasound Database. The Ultrasound Controller collects data about monitored FRS replica sets and stores the information in the Ultrasound database. The database runs on a server with MSDE or SQL Server 2000 with Service Pack 3a or above applied. Figure 16.13 illustrates a deployment topology for monitoring FRS with MOM and Ultrasound.

CAUTION

As stated in the FRS Management Pack Guide, do not install either of the Ultrasound components on the MOM database or on MOM management servers. This will avoid contention between the MOM and Ultrasound components.

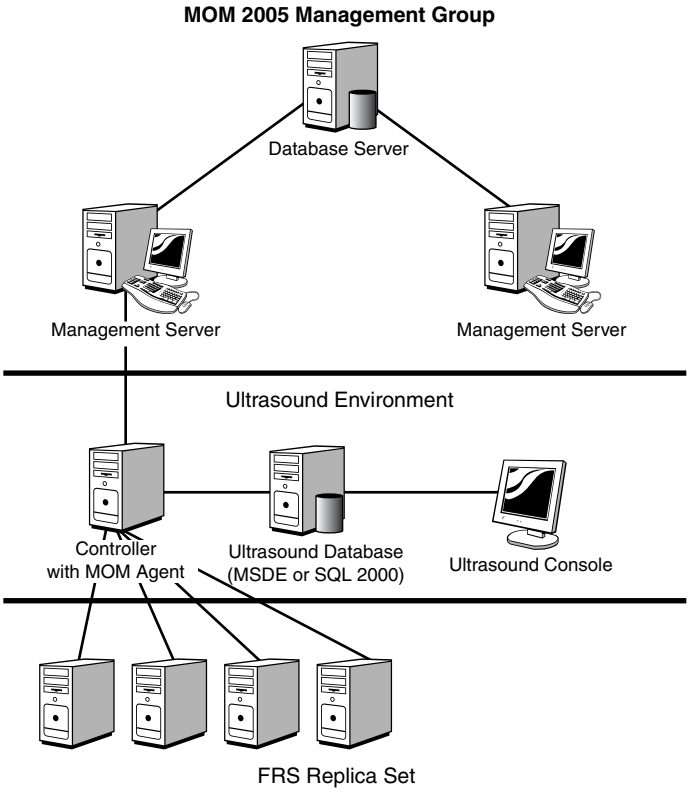


FIGURE 16.13 FRS with Ultrasound Deployment Topology.

The Windows File Replication Service Management Pack uses Ultrasound to gather information for monitoring FRS. After deploying Ultrasound, deploy a MOM agent to the Ultrasound server; then follow the procedures documented in Chapter 13 to extract and install the FRS management pack into your MOM environment. The extract includes one management pack—Microsoft Windows File Replication Service.akm. The management pack contains various tasks and reports.

Tasks

The FRS management pack includes a number of tasks, several of which you can use to diagnose and resolve FRS issues for your domain controllers:

- Ultrasound service—Starting or stopping of the Ultrasound service
- FRS service—Starting or stopping of the FRS service

Reports
The Microsoft Windows FRS Report group provides reports including

- Ultrasound - Frequently Detected Issues: Summary
- Ultrasound - Frequently Detected Issues: Most Problematic Replica Sets
- Ultrasound - Frequently Detected Issues: Most Problematic Members
- Ultrasound - Frequently Detected Issues: Most Problematic Connections

The FRS management pack pushes rules to the server running the Ultrasound Controller. These rules run scripts that gather information from the Ultrasound database. The collected information is provided to the MOM 2005 management server.

Scheduling FRS Health Events A MOM event is created if any unhealthy object such as a recurring failure to replicate between members is occurring and found by Ultrasound. The MOM events appear in the Operator console and are viewed to determine results of tasks or other MOM-related events. By default, the script to check for unhealthy objects runs every 2 hours. This configuration can be changed using the following procedure:

1. Open the Administrator console to Management Packs \ Rule Groups \ Microsoft Windows File Replication Service \ FRS Ultrasound \ FRS Health Details \ Event Rules \ Script \ Gathers FRS Health Details from Ultrasound. Right-click and choose Properties.
2. Click on the Data Provider tab and select Modify.
3. On the Timed Event Provider Properties page change the timed event from 2 hours to meet your environment's requirements.

Checking Controller Status A second script polls the Ultrasound database for status of the Ultrasound controller itself. This script runs with a default configuration of every 30 minutes, which you can change through the following steps:

1. Open the Administrator console to Management Packs \ Rule Groups \ Microsoft Windows File Replication Service \ FRS Ultrasound \ FRS Ultrasound Controller \ Event Rules \ Script \ Gathers Ultrasound Controller Status. Right-click and choose Properties.
2. Click on the Data Provider tab and select Modify.
3. On the Timed Event Provider Properties page change the timed event from 30 minutes to a different interval.

Monitoring Group Policy

Group policy is a powerful tool allowing administrators to easily specify a wide range of security and configuration settings for users and computers throughout the Active Directory. Two group policies exist in every AD domain by default: the default domain

policy and the default domain controller policy. These policies specify, among other things, the most important security settings for the domain. Additional group policies can be applied to specific sites, organizational units, or computers within the domain.

Group Policy is an integral service of Active Directory. In an Active Directory environment, you should monitor the application of group policies to ensure that your security policy and other configurations are correctly applied. The Group Policy MP answers questions such as:

- Is policy information being located and retrieved successfully from Active Directory?—Group Policy can be used for a variety of items including controlling desktop settings and deploying software. If the policy information is not located and successfully retrieved from Active Directory it will not function correctly.
- Is the Resultant Set of Policies (RSOP) being evaluated and logged?—Both the RSOP utility and the Group Policy Results feature of the Group Policy Management console cannot provide detail if the RSOP cannot be evaluated and logged correctly.
- Is the Security Client Side Extension (SCE) applying security policies successfully?—Failures on application of Group Policy can also occur on the client side in situations where the client cannot reach the security policy files on the domain controllers. MOM can identify Group Policy failures and can point to next steps required to debug them, including investigation of log files.

  Additional details on debugging and resolving Group Policy issues by using log files is available on the Microsoft TechNet website at http://technet2.microsoft.com/WindowsServer; search on "Fixing Group Policy problems by using log files: Group Policy."

Locate, Download, Install

From the Management Pack Catalog download the Group Policy Management Pack for MOM 2005/2000. The Windows Group Policy management pack (GPMP) is currently a MOM 2000 management pack.

The extract from the package includes one management pack—GPMP.AKM. Because the management pack was written for MOM 2000, it does not include reports or tasks. Additionally, there is no management pack guide for the Group Policy Management Pack.

Much of the GPMP does not work on an agentless managed server. After adding the Group Policy management pack to MOM 2005, verify that agents are installed on the servers you will be monitoring with the Group Policy Management Pack. If agents have not been deployed, install the MOM agent for MOM to push the Group Policy Management Pack to those systems. The GPMP is intended for deployment to key infrastructure servers. Because it requires the MOM agent, the management pack is not suitable to deploy to large numbers of client computers such as laptops and desktops.

The GPMP only monitors the application of Group Policy and client-side extensions on Windows Server 2003; it does not apply to Windows 2000 or Windows XP systems. As

Group Policy utilizes Active Directory and DNS, the Group Policy Management Pack should be used in conjunction with the Active Directory and DNS Management Packs.

Rules and Alerts

The management pack provides an extensive set of event rules to monitor Group Policy processing. Group Policy processing is controlled by the Group Policy Engine, which resides within userenv.dll.

More Information on Group Policy Processing

For more information about Group Policy processing see the Microsoft Windows TechCenter at http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef. Navigate to Technologies Collections and then Group Policy Collection under Group Policy Components; within Administrative Templates Extension Technical Reference, select How Administrative Templates Extension Works.

The rules in the Group Policy Machine and User Processing rule group monitor the operation of the Group Policy engine, whereas those in the Group Policy Client Side Extension Processing rule groups monitor operation of specific extensions. Not all client-side extensions are included in the Group Policy Management Pack. Monitored extensions are Disk Quota, Folder Redirection, Registry, Scripts, Security, and Software Installation. One of the more valuable aspects of the GPMP is the extensive knowledge base it makes available for Group Policy events.

Group Policy provides a large amount of the functionality available within Active Directory; if deployed within your environment its health can be critical to your clients' and servers' functionality. The GPMP provides the ability to monitor the Group Policy functionality within your Active Directory environment.

Configuring the Group Policy Management Pack

Userenv.dll contains Group Policy engine code and is called whenever policy settings are processed. The Group Policy Management Pack contains an extensive set of rules for UserEnv events. The Active Directory management pack also contains a UserEnv event rule. You should disable the Active Directory - UserEnv Processing rule groups if you are using the GPMP. You may also choose to disable rule groups within the management pack for specific client-side extensions not used in your environment.

Third-Party Tools

The components and services addressed by the management packs we have discussed play important roles in the enterprise environment, and a number of third-party management packs also target these services. We did not attempt to discuss any third-party MPs in this chapter but focused exclusively on those developed by Microsoft. Information about management packs, including those provided by third parties, is available at the Management Pack Catalog, http://go.microsoft.com/fwlink/?linkid=43970.

Summary

This chapter addressed how to effectively manage your directory services. We discussed the Active Directory, Windows Server Base OS, DNS, FRS, and Group Policy management packs, which can help your organization manage not only your Active Directory but also services that Active Directory depends on.

One of the many applications that depend on Active Directory is Microsoft Exchange. In the next chapter, we discuss using MOM 2005 to manage your Microsoft messaging environment.

CHAPTER 17

Managing Microsoft Messaging

IN THIS CHAPTER

- Monitoring Messaging with MOM
- Exchange Server 2000 and 2003 Management Pack
- Exchange Server Best Practices Analyzer Management Pack
- Microsoft Operations Manager 2005 SLA Scorecard for Exchange
- Additional Management Packs to Monitor Messaging
- Third-Party Tools

Messaging is a primary communication mechanism between employees and often part of workflow applications. However, it is often overlooked as a core business application. Just think back to the last time there was a problem with email—how long did it take for the user community to notify the help desk or other support personnel? Reaction to a malfunctioning communication system is almost immediate, and messaging's high visibility makes it crucial to be aware of issues that may cause interruptions or outages.

The major challenges in monitoring messaging solutions involve a number of different factors:

- Most email users are heavily dependent on it for communication. Email users often have a different perspective than administrators. They notice the effects—such as a slow response—although there are different causes for such behavior, such as system problems or a local virus. In most organizations users consider email to be a core requirement in performing their job function.
- Identifying performance trends on email environments is necessary for providing a method to address potential server limitations, preferably before they impact the end-user.
- As businesses integrate email into their workflow, malfunctioning email directly impacts a business's capability to function.
- Messaging is often distributed across multiple servers and physically distributed to many remote locations. Connectivity between locations and the capability to

monitor multiple servers from a single user interface is critical to effectively monitoring a messaging environment.

- Email has infrastructure-related dependencies; issues occurring in other areas of the infrastructure may impact email. For example, Microsoft Exchange relies on Active Directory—if Active Directory is not functioning, Exchange also is not functional. Email is generally a server-based solution, so if the server running Exchange is not functional, Exchange is not functional.

Information on Active Directory

Chapter 16, "Managing Directory Services," includes information for managing your Active Directory infrastructure.

This chapter provides direction to assist in monitoring and resolving issues before problems impact your messaging environment.

Monitoring Messaging with MOM

As you investigate MOM 2005's capabilities to manage your messaging infrastructure, keep in mind that a number of management packs exist that focus on different facets of messaging, although no individual management pack will address all aspects of managing your messaging environment. Various management packs from Microsoft and third-party vendors provide monitoring capabilities; the ones you choose to implement should depend on your specific requirements.

For Exchange 2000 and 2003 environments, the Exchange Server 2000 and 2003 Management Pack provides a majority of monitoring functionalities. You should also choose to implement the Exchange Server Best Practices Analyzer Management Pack, and the Exchange Intelligent Message Filter (IMF) Management Pack if you are using an earlier version of Exchange than Exchange 2003 Service Pack 2 (SP2). These management packs provide other capabilities for monitoring messaging. The management packs for monitoring Exchange are accessible at the Management Pack Catalog at http://go.microsoft.com/fwlink/?linkid=43970.

Exchange Server 2000 and 2003 Management Pack

The Exchange Server 2000 and 2003 Management Pack monitors your Exchange environment, helping you proactively address issues rather than react to problems as they occur. This management pack monitors whether the Exchange services are running, the databases are mounted, the mail is smoothly flowing in the environment, and Exchange is correctly configured. The Exchange management pack (MP) monitors the performance, availability, and security of your Exchange servers.

The Exchange MP monitors and maintains messaging resources to help you to meet the challenges inherent in managing messaging solutions. Making sure that your Exchange servers are operating reliably is a key concept for daily operations. It is best to approach monitoring for Exchange systematically, based on the principles outlined in the Microsoft Operations Framework (MOF) (http://go.microsoft.com/fwlink/?linkid=25297), which we introduced in Chapter 1, "Operations Management Basics."

Managing Messaging with the Exchange Management Pack

A significant part of daily operations in Information Technology (IT) is monitoring system health. Monitoring can verify that Service Level Agreements (SLAs) are met and lets you proactively detect and address issues in your Exchange organization before they impact the user community. Monitoring can also help to estimate future demands based on usage patterns and other performance data.

Do your users complain that email is slow? MOM can investigate and proactively monitor this issue, improving the user experience. As discussed in the "Checking Mail with Synthetic Transactions" section later in this chapter, the Exchange management pack checks for latency in message delivery and lets you know whether users are experiencing delays receiving their email.

Other areas where the Exchange management pack proactively identifies issues before they impact users include

- Monitoring free disk space on the Exchange drives—If the Exchange server runs out of disk space on its data or log drive, the server crashes—with your options limited to recovering from backup or contacting Microsoft support to attempt recovery of your server. MOM helps you by monitoring available space and notifying you when disk levels are critically low.
- Watching for corruptions in the database files—MOM monitors the results of online defragmentation, notifying you if corrupt pages are found during the defragmentation process.
- Warning you if your Exchange server is running out of memory and/or in a state where server instability may occur.

An additional challenge is managing a multiple server messaging configuration with a single console. Here MOM 2005 provides significant benefits in managing messaging because all the messaging servers in your environment can be monitored from one console, with their status displayed in a single Diagram view in the MOM 2005 Operator console. Figure 17.1 shows the Exchange Diagram view.

The Operator console can also show the state of all Exchange servers in a State view, shown in Figure 17.2.

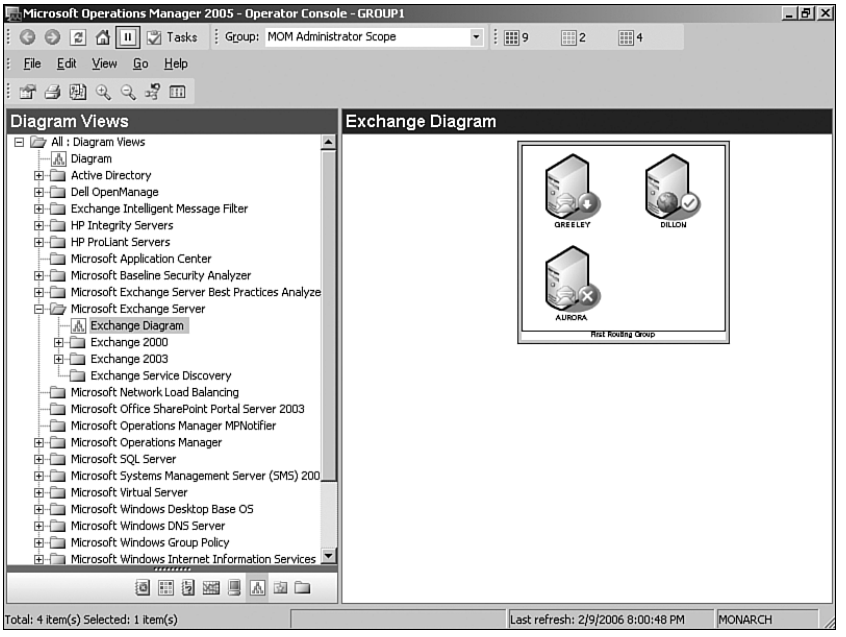


FIGURE 17.1 Operator Console Exchange Diagram view.

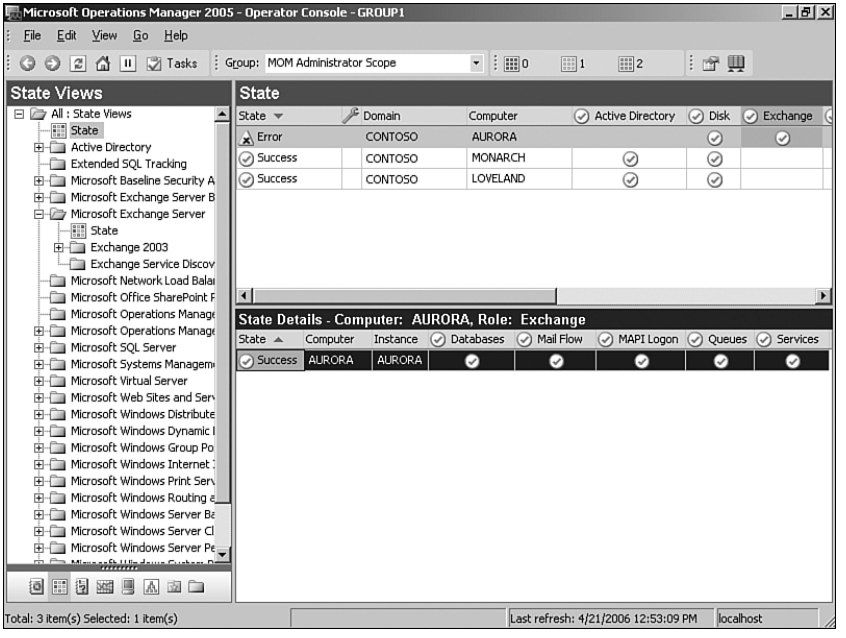


FIGURE 17.2 Operator Console Exchange State View.

You can use either of these views for identifying potential Exchange server issues so that they can be promptly diagnosed and resolved.

Finally, MOM 2005 monitors the services Exchange depends on. As discussed in Chapter 16, management packs are available for DNS (Domain Name System), Active Directory, and other components necessary for a solid messaging environment.

Now that we understand some of the benefits of the Exchange management pack in monitoring messaging, let's look at the steps required for installing and configuring the management pack itself.

Locate, Download, Install

From the Management Pack Catalog download the Exchange Server 2000 and 2003 Management Pack.

Downloading Management Packs from the Management Pack Catalog

Be sure to use the Management Pack Catalog to obtain management packs for MOM 2005. Although some management packs are on the MOM 2005 installation CD, Microsoft's Management Pack Catalog always has the most recent version.

After downloading the package, follow the procedures documented in Chapter 13, "Administering Management Packs," to extract and install the management pack. The extract includes several significant files:

- MicrosoftExchange2000Server.akm—The management pack for Exchange 2000
- MicrosoftExchangeServer2003.akm—The management pack for Exchange 2003
- MicrosoftExchangeServerReports.xml—Report definitions

Be sure to choose only the management pack(s) appropriate for the version(s) of Exchange you have in your environment. After successfully executing the Management Pack Import/Export Wizard, the corresponding Exchange server management pack is installed into your MOM 2005 management group. Because reports are included in this management pack, choose the Import Management Packs and Reports option during the management pack import process if you are using MOM Reporting.

Microsoft provides a guide for this management pack, which is the Exchange Server Management Pack Guide. Microsoft's management pack guides are available at http://go.microsoft.com/fwlink/?linkid=49776 and are often stored with the contents of the downloaded management packs.

If agents are not deployed onto the Exchange servers, install the MOM agent on your Exchange servers before deploying the Exchange Server management pack. The Exchange management pack is not designed to fully support agentless monitoring, as described in the next section. Information on installing the MOM agent can be found in Chapter 9, "Installing and Configuring Agents."

Agentless Monitoring

A subset of the functionality in the Exchange management pack works with agentless configurations. Agentless monitoring requires that you manually add each server to the appropriate computer group, based on its role. These include the Microsoft Exchange Server 2003 Back-End, Microsoft Exchange Server 2003 Front-End, Microsoft Exchange 2000 Server Back-End, and Microsoft Exchange 2000 Server Front-End roles.

The following features are available without an installed agent:

- Event collection
- Event monitoring
- Server performance collection
- Server performance threshold monitoring

The following features are available only with an installed agent:

- Client monitoring
- Database configuration monitoring
- Database health
- Disk space monitoring
- Health and availability monitoring
- Server performance collection
- Service availability
- Service discovery
- Service Pack compliance
- State monitoring

Configuring the Exchange Management Pack

Without making any configuration changes, the Exchange management pack provides only a basic level of functionality for event monitoring and Exchange performance metrics. Microsoft provides a configuration wizard for the management pack, giving it increased monitoring capabilities including monitoring mail-flow and advanced functionalities. The Exchange 2003 Management Pack Configuration Wizard provides a user interface for identifying and making configuration changes in your Exchange monitoring environment.

Exchange supports a front-end and back-end server capability, which is typically used in larger production environments. Front-end servers provide access to email via Outlook Web Access, Outlook Mobile Access, and ActiveSync. Front-end servers do not actually

have mailboxes associated with them; they are primarily used to offload work from the back-end servers, which store the user mailbox information. If your environment utilizes front-end servers, specific steps are required for MOM to monitor these servers.

Exchange Front-End Server Considerations

When using MOM 2005 to monitor Exchange front-end servers, there are a number of security recommendations to implement before running the configuration wizard:

- Run IIS Lockdown on all Exchange Front-End servers with IIS 5.1 or earlier. IIS Lockdown assists in making Internet-facing servers less susceptible to malicious attacks. For details on the IIS Lockdown tool, refer to KB article #325864. This article can be located at http://support.microsoft.com/kb/325864/.
- Secure the message tracking log files. The default location of these files is *%ProgramFiles%*\exchsrvr\servername.log. This folder is shared to allow Exchange administrators to view information from any Exchange System Manager Console.

Restricting Access to the servername.log Share

Restrict the share permissions for the servername.log share so that the Everyone group does not have access to this share. In Exchange 2003, this share is accessible only by administrators by default.

- The Simple Mail Transfer Protocol (SMTP) directories should be located on an NT File System (NTFS) partition, although no specific security settings are required. By default, the SMTP directory is located under the Exchange server directory.

Locating the SMTP Directory

As an example, an Exchange server installed to the default location (*%ProgramFiles%*\exchsrvr) has a default SMTP directory of *%ProgramFiles%*\exchsrvr\mailroot\vsi 1\Queue. To determine the location of the SMTP directory on your Exchange servers, launch the Exchange System Manager and browse to Servers \ <*servername*> \ Protocols \ SMTP \ Default SMTP Virtual Server. Right-click on Default SMTP Virtual Server and select Properties on the Message tab. The SMTP directory for the server is the Queue directory listed on this page.

  If the SMTP directories are not on an NTFS partition, convert the partition to NTFS or move the SMTP directory to an NTFS-formatted drive. When SMTP logging is enabled for MOM, the logs can grow quickly; large environments report growth of more than 250MB per day. You may want to move these directories to a drive with significant free space.

- Verify that SMTP cannot perform anonymous relay. The anonymous relays configuration setting is found in the Exchange System Manager under Servers \ <*servername*> \ Protocols \ SMTP \ Default SMTP Virtual Server \ Properties \ Access tab \ Relay.

There are several steps to configure the front-end server monitoring functionality for your Exchange front-end servers. These include

- Configuring SSL for all Microsoft Outlook Web Access (OWA)
- Activating forms-based authentication
- Configuring Outlook Mobile Access if it will be used in your environment
- Applying specific registry changes to the Exchange server

Most of these configurations are common configurations and may already be in place in your environment.

Configuring SSL To configure SSL on your servers, perform the following steps:

1. Obtain a web server certificate and apply it to the Exchange virtual website. Web server certificates can be purchased from certificate authorities such as Verisign or Thawte, or you can create your own Active Directory certificate server. If you use your own Active Directory certificate server, add the Certificate Authority certificate to the list of trusted roots.

Configuring SSL

For details on the specific steps to configure SSL, refer to the Exchange Server 2003 and Exchange 2000 Server Front-End and Back-End Topology Guide. The guide is found with the Microsoft Exchange TechCenter, and you can access it at http://www.microsoft.com/technet; in the left-hand pane select Products and Technologies, on the Product and Technologies page click on Exchange Server TechCenter; then in the Exchange 2003 section of the TechCenter choose Exchange 2003 Technical Documentation Library and then select the Front-End and Back-End Topology For Exchange Server 2003 and Exchange 2000 Server article.

2. Within the IIS configuration for each virtual directory, enable the Require Secure Channel option. Access the properties of each virtual directory, going to the Directory Security tab, Secure Communications, Edit, and check the option to Require Secure Channel. The default virtual directory names are Exchange, Microsoft-Server-ActiveSync, and OMA.

Activating Forms-Based Authentication Exchange 2003 supports a new logon security feature for OWA that is initially disabled in Exchange 2003. To monitor OWA, activate forms-based authentication on your Exchange front-end servers. This configuration is in the Exchange System Manager under Protocols \ HTTP \ Exchange Virtual Server\ Properties \ Settings tab. Check the Enable Forms Based Authentication option. Forms-based authentication requires SSL which was discussed in the "Configuring SSL" section earlier in this chapter.

Configuring Outlook Mobile Access Only front-end server configurations can monitor Outlook Mobile Access. The front-end server answers Outlook Moble Access (OMA) requests and requests information from the back-end server. If you want to monitor the back-end servers' OMA functionality you can do so from the front-end servers themselves; add the URLs to the OMA registry setting, which is discussed in the "Applying Registry Changes" section later in this chapter.

OMA is not enabled by default in Exchange 2003. If you are testing OMA, verify that it is activated in the Global Settings of the Exchange environment. This configuration is available within the Exchange System Manager under Global Settings. To activate OMA, check the Enable Outlook Mobile Access option.

Information on Configuring OMA

Additional details on OMA and its configuration are available in the Exchange Server Deployment Guide at http://go.microsoft.com/fwlink/?linkid=21768 in the "How to Enable or Disable Outlook Mobile Access at the Organizational Level" section.

Applying Registry Changes As discussed in the "Exchange Front-End Server Considerations" section earlier in this chapter, Exchange front-end servers require SSL configuration and forms-based authentication to function with MOM 2005. There are registry settings specifying what will be monitored on those servers. The registry values are found in the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange MOM\FEMonitoring\<*front-end servername*> key on the Exchange front-end server, created by the Exchange Management Pack Configuration Wizard. If your organization has multiple front-end servers that you want to monitor, you would make these changes on each front-end server. Table 17.1 lists the three major configurations, using the contoso.com domain as an example.

TABLE 17.1 Exchange Front-End Monitoring Configurations

Role	Key Name	Value	Sample Content
OWA	CustomUrls	String	https://mail.contoso.com/exchange
OMA	CustomOmaUrls	String	https://mail.contoso.com/oma
ActiveSync	CustomEasUrls	String	https://mail.contoso.com/Microsoft-Server-ActiveSync

Multiple entries can be listed by putting a comma between the URLs. An example of this for OMA would be

```
https://mail.contoso.com/oma, https://mail.contoso.com/mobile
```

Using the Configuration Wizard

Microsoft provides the Exchange Management Pack Configuration Wizard to assist in configuring the Exchange management pack. The configuration wizard simplifies configuration of your Exchange environment. The Microsoft Exchange Server Management Pack

Configuration Wizard is available for download at http://go.microsoft.com/fwlink/?linkid=35942. You can use the Exchange 2003 Management Pack Configuration Wizard with Exchange 2000 servers as well. There is no separate configuration utility download for Exchange 2000 servers.

The Exchange 2003 Management Pack Configuration Wizard configures items such as test mailboxes, message tracking, and what services should be monitored using MOM.

Prerequisites There are three prerequisites to installing the Exchange Configuration Wizard:

1. Install the MOM agent on all Exchange servers in your environment that you want to monitor. The Exchange Wizard cannot configure Exchange servers without an installed MOM agent; the error message you would receive in this instance is shown in Figure 17.3.

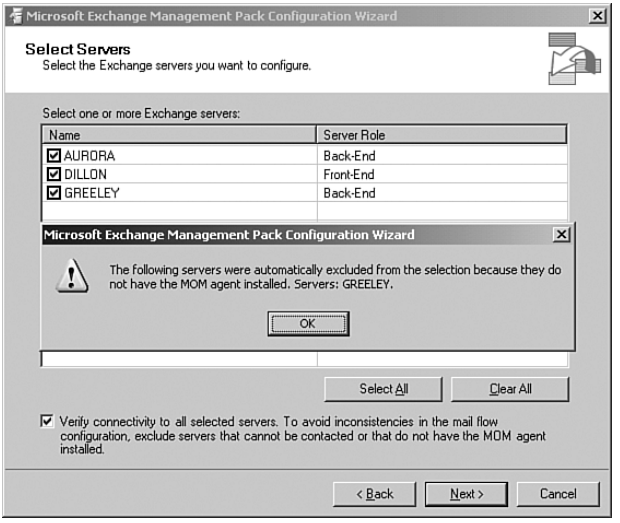


FIGURE 17.3 Running the Exchange Configuration Wizard without an installed agent.

2. Install the management pack as discussed in Chapter 13.
3. Install the Exchange System Manager on your management server(s). To install the Exchange System Manager insert the Exchange Server 2003 CD, select Exchange Deployment Tools, and click on Install Exchange System Management Tools Only on the Welcome to the Exchange Server Deployment Tools dialog box.

Installing the Wizard To install the wizard, perform the following procedure:

1. Run the package you downloaded from the Microsoft download website to extract the configapp.msi configuration wizard install utility.
2. Run the extracted configapp.msi file, installing the wizard.

3. The wizard is now accessible on the Start menu under the Exchange Management Pack/Exchange Management Pack Configuration Wizard.

Where to Install the Exchange Management Pack Configuration Wizard

Microsoft suggests installing the configuration wizard on an existing Exchange server. If you take this approach be sure to make a note of the server because you will rerun the wizard if you add or remove Exchange servers in your environment.

We recommend installing the Exchange System Manager (ESM) and the configuration wizard on the same management server. This gives you a consistent location to rerun the wizard from. It also avoids logging in to the Exchange servers to run the wizard (in some organizations Exchange administrators may frown on the MOM administrator logging in to their servers).

Configuring Servers The configuration wizard lets you select servers to configure based on the administrative groups you want to monitor. The wizard automates the process to configure advanced monitoring for front-end servers, message tracking, service monitoring, mailbox availability, and mail flow. Figure 17.4 shows the details of the wizard configuration screen.

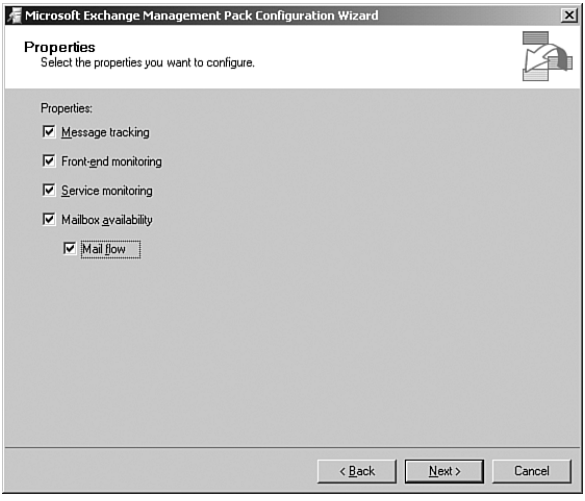


FIGURE 17.4 Custom configuration with the Microsoft Exchange Management Pack Configuration Wizard.

Index Must Be Greater Than or Equal To Zero Error

If you receive an error when running the wizard that states "Index (zero based) must be greater than or equal to zero and less than the size of the argument list," a hotfix needs to be applied to the Exchange server. This hotfix is included in Windows 2003

SP1 and is also resolved in the current version of the wizard available for download. Information related to this error is available at http://support.microsoft.com/kb/835763/.

Enabling Exchange Diagrams

The Exchange configuration wizard addresses most of the configuration changes needed to effectively use the Exchange management pack. There is one remaining configuration you may want to investigate. Within the Operator console there is an Exchange topology Diagram view that is populated only after you identify which server in your environment performs Exchange Topology Discovery. To use the Exchange topology diagram in the MOM 2005 Operator console make the following configuration changes:

1. Identify an Exchange server that will perform topology discovery. This system can be any Exchange 2000 or 2003 server in the Active Directory forest.
2. In the MOM 2005 Administrator console, under Administration \ Computers \ All Computers, right-click on the computer that you put into the Microsoft Exchange Topology Discovery Computers group. On the Properties page, select the Security tab and clear the Use Global Settings and Prevent Agent from Proxying for Other Computers or Network Devices check boxes, as shown in Figure 17.5.

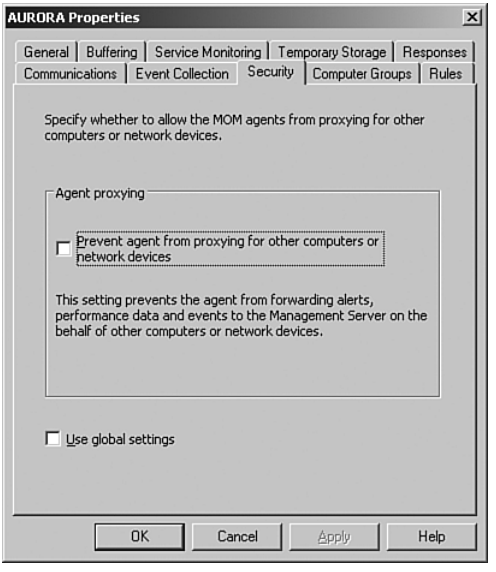


FIGURE 17.5 Computer proxy settings in the Microsoft Exchange Topology Discovery Computers group.

3. In the Administrator console, navigate to Management Packs \ Computer Groups \ Microsoft Exchange Topology Discovery Computers. Add the Exchange server that you want to designate.

By adding a computer to this group, you are applying the Launch Exchange Topology Discovery rule (part of the Exchange Topology Discovery rule group) that runs the Exchange - Topology Discovery script. This script collects topology and server configuration information to populate the MOM service discovery tables that are used by the Exchange Diagram view.

4. Click OK on the Microsoft Exchange Topology Discovery Computers Properties page to save your changes.

Configuration Summary

The Exchange management pack is one of the more complicated management packs from an installation and configuration perspective. Specific steps are required to configure all of the Exchange servers in your environment using the configuration wizard. As already mentioned, configuration is required to monitor front-end servers and to activate the Exchange Diagram view.

Common Configuration Issues with the Exchange Server Management Pack

Microsoft has provided a list of the top three configuration issues with the Exchange Server Management Pack:

- Missing 9986 Events in MOM: Configuration Wizard error, Error: Cannot configure the mailbox access account on computer <*servername*>. This configuration can only be made after the Exchange MOM event 9986 is registered by MOM.
- MAPI Logon Verification Script Errors: Multiple potential error messages, including MAPI_E_NOT_FOUND, MAPI_E_LOGON_FAILED, and MAPI_E_NOT_INITIALIZED.
- Outlook Web Access Monitoring: Errors reported within MOM indicates that the Outlook Web Access logon failed.

Details on these three issues and their resolutions are available at http://www.microsoft.com/technet/prodtechnol/exchange/2003/empconfig.mspx.

Rules and Alerts

The Exchange Server 2000 and 2003 Management Pack tracks an incredible amount of information ranging from specific component functionality such as OWA to connectivity with your Active Directory servers. Let's take a closer look at some of the rules and alerts available as we discuss synthetic transactions and OMA tuning.

Checking Mail with Synthetic Transactions

Exchange can generate synthetic transactions that send mail between your email servers. After you use the Exchange configuration wizard (discussed in the "Using the Configuration Wizard" section earlier in this chapter) to configure mail flow, MOM tracks whether mail is flowing and the latency associated with each email message sent.

For example, in Figure 17.6 the Aurora mail server sends an email to the Greeley server (both are back-end Exchange servers). If the outbound queue on Aurora is stopped, the message continues to sit in the Aurora queue. Because Greeley is expecting an email message that it does not receive, it notifies the management server that it has not received the email. After a (configurable) period of time, another email is sent from the Aurora server.

The rule monitoring this particular situation is found under Management Packs \ Rule Groups \ Microsoft Exchange Server \ Exchange 2003 \ Availability and State Monitoring \ Verify Mail Flow \ Event Rules and is the Error: Mail flow message not received rule. If the outbound queue on Aurora is restarted and both email messages are delivered, the first email message indicates significantly higher latency than the second. Figure 17.6 shows an example of the mail flow.

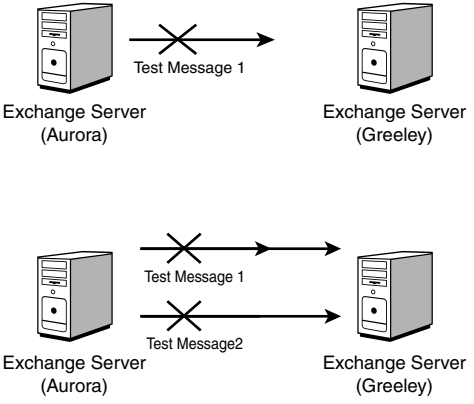


FIGURE 17.6 Mail flow testing between the Aurora and Greeley servers.

Synthetic transactions provide a method to determine latency within your Exchange environment, giving you insight into email flow from a user's perspective.

Tuning OMA

You may want to change the thresholds generating alerts for conditions in your OMA environment. For example, in versions of the Exchange MP prior to the release of Exchange 2003 SP2, alerts were often issued stating that Outlook Mobile Access was not responding within 60 seconds. The default threshold in the rule had been accidentally defined as 60 milliseconds instead of 60 seconds (not too many OMA servers respond quite that fast!). If your environment does not need OMA to respond within 60 milliseconds, you will want to "tune," or change the rule criteria to fit your environment. The specific rule to tune is shown in the Alert properties in the Operations console. As shown in Figure 17.7 this value is now defaulted to 60000 milliseconds, which equal 60 seconds.

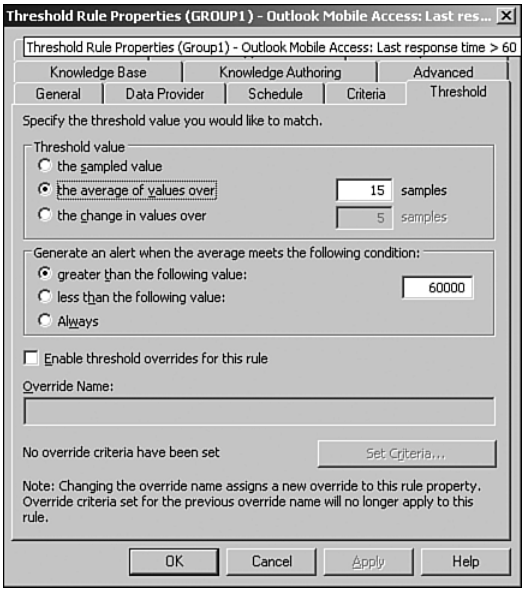


FIGURE 17.7 OMA Threshold Rule properties.

Determining the Rule Creating an Alert

To identify which rule is firing a particular alert, the location of the rule is always specified in the bottom-right section of the properties page of the alert in the Operator console.

To modify this rule, perform the following steps:

1. In the Administrator console, navigate to Management Packs \ Rule Groups \ Microsoft Exchange Server \ Exchange 2003 \ Health Monitoring and Performance Thresholds \ Server Performance Thresholds \ Performance Rules.
2. In the Details pane, right-click on the Outlook Mobile Access: Last response time > 60 seconds and choose Properties.
3. Select the Threshold tab and enter the new value in the Generate an Alert When the Average Meets the Following Condition - Greater Than the Following Value field. This value is in milliseconds not seconds.
4. Click OK to save your changes.

As always when modifying a management pack, be sure to commit configuration changes. This is described in Chapter 13.

Tuning the Exchange Queue Thresholds

The Exchange management pack often requires tuning for your particular Exchange environment. Microsoft provides default values for thresholds appropriate for most environments, but you may need to tune these based on your server volume. The management pack includes default thresholds for the various queues used in Exchange including those related to SMTP and the Message Transfer Agent (MTA). These rules are located within Management Packs \ Microsoft Exchange Server \ Exchange 2003 \ Health Monitoring and Performance Thresholds \ Mail Queue Thresholds and State Monitoring \ Performance Rules. The rules in this folder generate alerts when they detect a disruption in mail flow. Some rules in this folder that are commonly tuned related to SMTP include

- Mailbox Store: Send Queue > 25 and Mailbox Store: Receive Queue > 25—These rules track the number of messages awaiting transfer (send queue) and those being received (receive queue). Both these rules and suggested tuning were discussed in Chapter 14, "Monitoring with MOM."
- Exchange 2003: SMTP: Categorizer Queue > 50—Number of messages in the categorizer queue.
- Exchange 2003: SMTP: Local Retry Queue > 50—Message queue for messages waiting to be delivered to the database that previously failed delivery.
- Exchange 2003: SMTP: Local Queue > 50—Queue of messages waiting for delivery to the Microsoft Exchange Information Store service.
- Exchange 2003: SMTP: Messages in SMTP Queue Directory > 500—Tracks the number of messages in the queue stored on the physical disk.
- Exchange 2003: SMTP: Messages Pending Routing > 50—Number of messages that are categorized but not routed.
- Exchange 2003: SMTP: Remote Queue > 500—Remote queues that send to other servers.
- Exchange 2003: SMTP: Remote Retry Queue > 500—Number of messages in the remote queue that cannot be sent to a destination server.

Some rules in this folder that are commonly tuned related to the MTA include:

- Exchange Information Store service Queue of Messages to MTA > 50—Number of messages in transit to the MSExchangeMTA.
- Information Store Queue of Messages from MTA > 25—Number of messages being sent from the MTA to the Exchange store.
- MTA Queue Length per Connection > 50—Outstanding messages queued for transfer to the database and the Pending Reroute queue.
- MTA Work Queue > 50—Number of messages not yet processed to completion by the MTA.

Exchange Intelligent Message Filter

Prior to Exchange Server 2003 Service Pack 2 the Exchange Intelligent Message Filter (IMF) was a separate download from the Microsoft website, with a corresponding management pack monitoring IMF functionality. The Exchange IMF management pack is no longer available; it was made obsolete with the release of Exchange 2003 Server SP2 and a corresponding release of the Exchange Server management pack. Service Pack 2 incorporates the IMF functionality into Exchange.

Exchange's IMF functionality is used to reduce the amount of Unsolicited Commercial Email (UCE), also known as *spam*. Spam is a significant technical issue; reports estimate that more than 50% of total email traffic is spam. The Intelligent Message Filter is built on Microsoft SmartScreen Technology, which uses an algorithm to determine whether email is legitimate or spam. SmartScreen essentially "learns" over time what is legitimate email and what is spam. The IMF allows you to determine whether to block these messages at the gateway or at the mailbox store.

The Exchange IMF management pack functionality, previously in a separate management pack, is now integrated into the Exchange management pack. Functionality was added in two areas:

- Management Packs \ Rule Groups \ Microsoft Exchange Server \ Exchange 2003 \ Performance Counter Logging Rules \ Exchange Utilization and Performance \ Intelligent Message Filter Statistics
- Management Packs \ Rule Groups \ Microsoft Exchange Server \ Exchange 2003 \ Exchange Event Monitoring \ Intelligent Message Filter

The Exchange management pack contains rules that collect UCE metrics, notifies you when there are message filter updates, and provides notification of critical or higher errors. The alerts and rules include

- Error Filtering a Message—If the IMF cannot filter a message, it places event number 7515 in the application log on the Exchange Server from the source of MSExchangeTransport. The management pack looks for this event and provides knowledge on potential causes for this issue, including corrupted or malformed messages.
- Error Updating the IMF—The IMF requires periodic updates to effectively filter spam. If the IMF cannot update itself, it places an event number 7514 in the Exchange server application log with a source of MSExchangeTransport. The management pack monitors for this event and provides a potential resolution.
- Performance Statistics—The IMF management pack also tracks performance statistics to let you know how many messages are being scanned for spam, how many messages are being flagged as spam, and what percent of the email messages are classified as spam.

The IMF functionality is based on SmartScreen technology, which does an excellent job in avoiding false positives (situations where a valid email is identified as spam). The IMF calculates a value called the Spam Confidence Level (SCL) for each message. The value of

the SCL ranges from 0 to 9, with the higher the value of the SCL the more likely the message is spam. Generally, messages ranked 8 or higher are almost always considered spam. Depending on the SCL value, Exchange can either block messages or move those messages to a user's Junk message folder (or both based on configuring different SCL values). Spam email negatively impacts users' perceptions of your messaging solution. Removal of spam from the environment while minimizing false positives can assist in providing a more positive messaging user experience.

Reports

The Exchange management pack includes a number of reports that can be used to provide configuration information and historical reports for trending purposes. The Exchange reports allow you to track items that can help identify bottlenecks and track usage of your Exchange server environment. Several issues associated with reports were resolved with the Exchange management pack released in conjunction with Exchange 2003 Service Pack 2.

The Exchange Disk Usage report provides average disk queue lengths including the highest average rate during a half-hour period and when that actual time frame is. This report (shown in Figure 17.8) provides information that will help you to identify potential disk bottlenecks and specific time frames when the Exchange environment may be heavily utilized.

Exchange Disk Usage

Microsoft Operations Manager 2005

Description 5/4/2006 4:56:23 PM

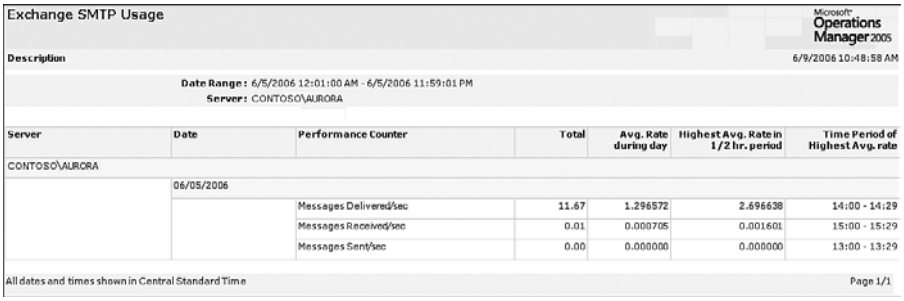
Date Range: 5/3/2006 4:56:14 PM - 5/4/2006 4:56:14 PM
Server: <ALL>

Server	Date	Disk	Performance Counter	Avg. Rate during day	Highest Avg. Rate in 1/2 hr. period	Time Period of Highest Avg. rate
CONTOSO\DILLON						
	05/03/2006					
		0 C:	Avg. Disk Queue Length	0.073084	0.091679	23:00 - 23:29
		0 C:	Disk Reads/sec	0.105044	1.059214	23:30 - 23:59
		0 C:	Disk Writes/sec	2.974259	3.186726	
		1 E:	Avg. Disk Queue Length	0.000005	0.000045	23:00 - 23:29
		1 E:	Disk Reads/sec	0.000000	0.000000	17:00 - 17:29
		1 E:	Disk Writes/sec	0.000980	0.009219	23:00 - 23:29
	05/04/2006					
		0 C:	Avg. Disk Queue Length	0.080238	0.085688	0:00 - 0:29
		0 C:	Disk Reads/sec	0.328458	0.435565	0:00 - 0:29
		0 C:	Disk Writes/sec	3.015908	3.057452	0:00 - 0:29
		1 E:	Avg. Disk Queue Length	0.000000	0.000000	0:00 - 0:29
		1 E:	Disk Reads/sec	0.000000	0.000000	0:00 - 0:29
		1 E:	Disk Writes/sec	0.000000	0.000000	0:00 - 0:29
CONTOSO\GREELEY						
	05/03/2006					
		0 C:	Avg. Disk Queue Length	0.045523	0.050480	19:30 - 19:59
		0 C:	Disk Reads/sec	0.002802	0.026153	19:00 - 19:29
		0 C:	Disk Writes/sec	2.630846	2.769840	22:30 - 22:59
		1 E:	Avg. Disk Queue Length	0.000000	0.000000	17:00 - 17:29
		1 E:	Disk Reads/sec	0.000000	0.000000	17:00 - 17:29
		1 E:	Disk Writes/sec	0.000000	0.000000	17:00 - 17:29
	05/04/2006					
		0 C:	Avg. Disk Queue Length	0.047902	0.049812	0:30 - 0:59
		0 C:	Disk Reads/sec	0.001130	0.001506	0:00 - 0:29

All dates and times shown in Central Standard Time Page 1/2

FIGURE 17.8 Exchange Disk Usage report for Dillon and Greeley servers.

The SMTP Usage Report, illustrated in Figure 17.9, shows information on SMTP traffic delivered, received, and sent by day. High values on this report indicate conditions such as heavy email utilization and can help identify specific times in the day when SMTP traffic is heaviest.



Exchange SMTP Usage

Microsoft Operations Manager 2005

Description 6/9/2006 10:48:58 AM

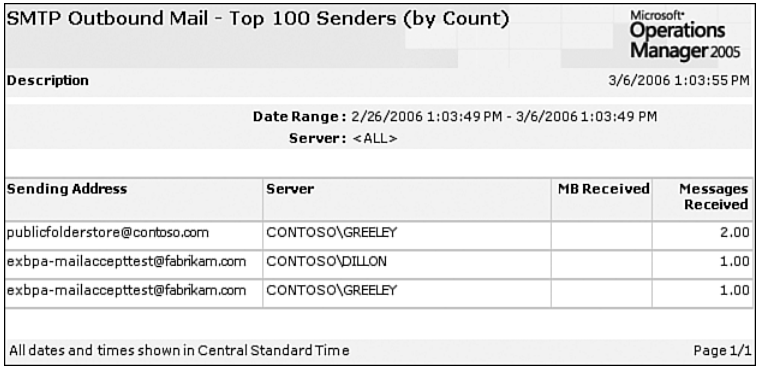
Date Range: 6/5/2006 12:01:00 AM - 6/5/2006 11:59:01 PM
Server: CONTOSO\AURORA

Server	Date	Performance Counter	Total	Avg. Rate during day	Highest Avg. Rate in 1/2 hr. period	Time Period of Highest Avg. rate
CONTOSO\AURORA						
	06/05/2006					
		Messages Delivered/sec	11.67	1.296572	2.696638	14:00 - 14:29
		Messages Received/sec	0.01	0.000705	0.001601	15:00 - 15:29
		Messages Sent/sec	0.00	0.000000	0.000000	13:00 - 13:29

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

FIGURE 17.9 Sample output from the SMTP Usage report.

Another tool to assist with managing messaging is the SMTP Outbound Mail - Top 100 Senders by Count report, illustrated in Figure 17.10. This report lists the users sending the most email, including public folder replication messages and messages from the Exchange Best Practices Analyzer. This report can also be used to determine whether specific user accounts are infected with viruses that use Microsoft Outlook to send out emails under the control of the intruder.



SMTP Outbound Mail - Top 100 Senders (by Count)

Microsoft Operations Manager 2005

Description 3/6/2006 1:03:55 PM

Date Range: 2/26/2006 1:03:49 PM - 3/6/2006 1:03:49 PM
Server: <ALL>

Sending Address	Server	MB Received	Messages Received
publicfolderstore@contoso.com	CONTOSO\GREELEY		2.00
exbpa-mailaccepttest@fabrikam.com	CONTOSO\DILLON		1.00
exbpa-mailaccepttest@fabrikam.com	CONTOSO\GREELEY		1.00

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

FIGURE 17.10 SMTP Outbound - Top 100 Senders (by count) report.

The Exchange management pack may be the most complex MOM 2005 management pack to deploy. Although this is a complicated management pack to implement and configure, it can go a long way towards meeting the challenges of monitoring your messaging environment. In the next section we cover additional management packs that assist in monitoring Exchange.

Exchange and the IIS Management Pack

If your environment has Exchange servers and also uses the IIS management pack, check to see whether you are receiving many Server Status =Unauthorized(401) events in the MOM 2005 Operator console. Depending on the size of your environment and the number of Exchange users there may be many of these messages, which are caused by browser checks within the Outlook Web Access system. These checks are written to the IIS logs and monitored by the MOM server. In a large Exchange environment this particular situation has been known to cause the MOM operational database to expand at a rate of 250MB per hour.

If you are receiving many of these messages on your system and they do not indicate an error condition, you can exclude your Exchange servers from being monitored by the IIS management pack. This is accomplished by going to Management Packs \ Computer Groups \ Microsoft Windows 2003 IIS Servers computer group and opening the properties page (if you are running Exchange on Windows 2000 IIS servers it would be under Management Packs \ Computer Groups \ Microsoft Windows 2000 IIS Servers). On the Exclude Computers tab, add the Exchange servers that are generating these events to the excluded servers list. After this is done recalculate your group memberships and commit the changes. This will effectively cause the IIS management pack rules to ignore the Exchange servers you listed.

Exchange Server Best Practices Analyzer Management Pack

The Microsoft Exchange development team developed the Exchange Best Practices Analyzer (ExBPA) to analyze your Exchange Server 2003 configurations and compare them with known best practices, giving you a report of action items to improve the performance and stability of your Exchange environment. The Exchange Server Best Practices Analyzer Management Pack works in conjunction with the ExBPA.

This management pack provides an automated method to report best practices and recommendations about your Exchange 2003 environment using the MOM 2005 interface. The Best Practices Analyzer (BPA) management pack is configured to run automatically on a daily basis at 11:20 p.m. The scheduled time can be changed as described in the "Scheduling the Exchange Best Practices Analyzer" section later in this chapter. The daily process reports the status of the Exchange Best Practices Analyzer using alerts to the management server. Figure 17.11 shows sample output.

Using the Exchange Server Best Practices Analyzer MP to Manage Messaging

By applying the changes recommended by the best practices analyzer you can increase performance and security and discover potential issues. Items identified by this management pack include the following:

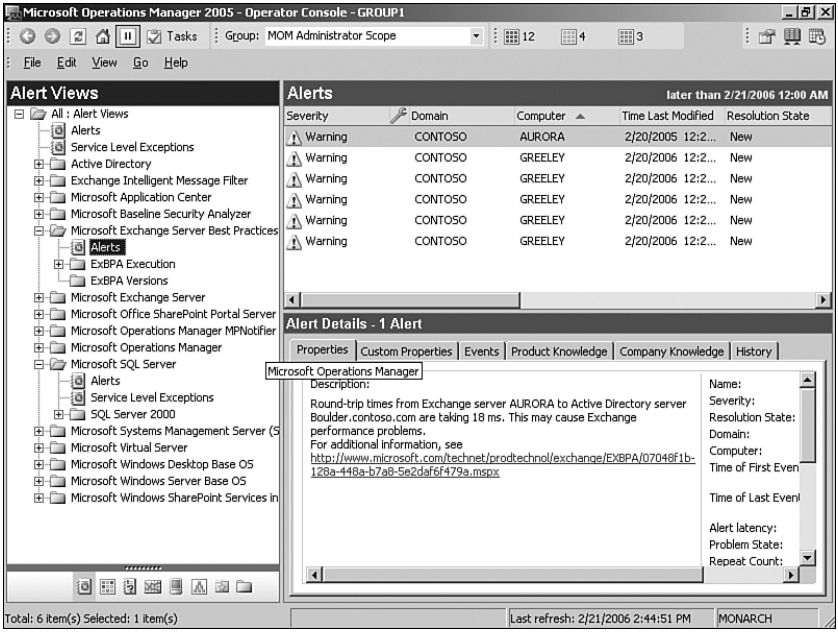


FIGURE 17.11 Sample errors and warnings filtered for only the Exchange Best Practices Analyzer tool.

- Is SSL configured for Exchange, OWA, OMA, and Active Sync components? SSL Encryption should be required on all websites utilizing basic authentication to prevent clear-text passwords from being sent over the network.
- Does the SMTP service have a separate drive to run on to enhance performance? A best practice approach is to move the SMTP service to another drive, increasing Exchange performance.
- What authentication methods are allowed on the SMTP virtual servers? Anonymous access, Basic Authentication, and Integrated Windows Authentication are all available options on the SMTP virtual server. This information could be important from a security perspective.
- What are the round-trip times from the Exchange servers to the Active Directory servers? (The BPA queries a Windows Management Instrumentation (WMI) class, which contains the round-trip time gathered through ping tests.) High round-trip times (defined by the BPA as greater than 10 milliseconds) between these servers can result in performance problems. A high round-trip time may indicate network latency or overutilization on the Exchange or Active Directory servers.
- Is circular logging enabled for the Exchange servers in the environment? As a general rule circular logging should only be used as an emergency measure when disk free space is critical.

- How long has it been since an Exchange database has been backed up? The Exchange Best Practices Analyzer watches to make sure that you have a backup strategy in place and that it is running on a regular basis.
- How many free page table entries (PTE) are available on the Exchange server? The PTE counter indicates a lack of available memory and can result in instability to the Exchange server(s).

Let's look at some of the details of the Exchange Best Practices Analyzer management pack.

Locate, Download, Install

Download and install the Exchange Server Best Practices Analyzer Management Pack; then follow the procedures documented in Chapter 13 to extract and install the management pack file. The extract includes the ExBPA.akm. No reports are included in this management pack, so use the Import Management Packs Only option with the management pack installation wizard.

Installation Notes for the Exchange Best Practices Analyzer

Prior to installing this management pack, the Best Practices Analyzer tool itself also needs to be downloaded to the management server. The ExBPA is available at: http://go.microsoft.com/fwlink/?linkid=34705.

The Microsoft .NET Framework 1.1 is required when installing the Exchange Server Best Practices Analyzer. Exchange 2003 includes the Microsoft .NET Framework, so no additional steps are required for Exchange 2003 servers. For earlier versions of Exchange or a MOM 2005 management server without .NET Framework 1.1 you will need to deploy the .NET Framework 1.1 before installing the ExBPA.

After adding the Exchange Server Best Practices Analyzer Management Pack to MOM 2005, verify that agents are deployed to the Exchange servers. The management pack requires these agents.

No management pack guide is currently available for the Exchange Best Practices Analyzer MP, although Microsoft provides a Readme.rtf file as part of the download package.

Configuring the Analyzer Tool

Install the Best Practices Analyzer tool on each Exchange server. This can be done manually on each server by logging in to the system and installing the ExBPA.msi file, or using the MOM Operator console. To deploy the tool through the MOM Operator console, perform the following tasks:

1. Create a share on the MOM Server to provide a Best Practices Analyzer deployment share and copy the ExBPA.msi into this directory.

Depending on your network topology you may need to create multiple shares on a per-site basis.

The ExBPA.msi file is approximately 4 megabytes (MB) in size, and the rules database is less than 1MB. The amount of data being sent should be taken into consideration when planning network utilization.

2. Configure the task in the MOM Administrator console under Management Packs \ Tasks \ Microsoft Exchange Server Best Practices Analyzer Tool.

   On the right-hand pane, right-click on the Install ExBPA and click on the Details tab. Double-click on the Parameter Default Values and change to the name of the MOM Server and sharename just created, for example: \\Monarch\ExchangeBA.

3. To run the task you just configured, open the Operator console, and on the right-hand side open the Microsoft Exchange Server Best Practices Analyzer Tool folder.

4. Select the servers to deploy the Analyzer to in the center pane (you can select multiple servers on the Events or Computers and Groups views), and click on the Install ExBPA tools on the right pane. Take the defaults and launch the program.

Checking Status of the ExBPA Analyzer Tool

You can check for successes or failures using the Task Status event view within the Operator console.

After installing the BPA on your servers you can use the MOM Operator console to execute the program for either an Exchange organization or an individual Exchange server.

To run the Best Practices Analyzer for your Exchange organization on an ad-hoc basis, select the server(s) on which to run the Analyzer in the Computers view and click on the Run ExBPA (Organization) tools on the right pane. Accept the defaults and launch the program. The Analyzer collects information about Admin groups and additional organization information.

The Best Practices Analyzer can also be run for servers rather than the Exchange organization. Select the servers on which to run the Analyzer in the center pane and click on the Run ExBPA (Server) tools on the right pane. The Analyzer collects information about the specific Exchange server's configuration.

Running an ad-hoc analysis either on the Exchange organization or the server does not impact the scheduled tasks that run these processes. Details on how to change scheduling for these is discussed later in the "Scheduling the Exchange Best Practices Analyzer" section.

Rules and Alerts

The Exchange Server Best Practices Analyzer Management Pack includes event rules that schedule running the ExBPA at the server and organizational level and notify of errors and warnings associated with ExBPA.

Most of the work performed by the Exchange Server Best Practices Analyzer tool is being done on the Exchange servers themselves using the ExBPA program. The MOM portion, which is the management pack, coordinates when the program executes and gathers the required information for the MOM server.

Scheduling the Exchange Best Practices Analyzer

The Exchange Best Practices Analyzer Management Pack schedules a daily run of the ExBPA on an organization level that runs at 11:10 p.m. This is configurable and is set in the Microsoft Exchange Server Best Practices Analyzer Tool \ ExBPA Org Rules \ Event Rules \ Daily ExBPA run (Organization) on the Data Provider tab.

The management pack also schedules a daily run of the ExBPA on a per-server basis at 11:20 p.m. You can change this setting in the Microsoft Exchange Server Best Practices Analyzer Tool \ ExBPA Scheduling \ Event Rules \ Daily ExBPA run (server) on the Data Provider tab.

Data Collection

The ExBPA management pack gathers data provided by the local executions of the ExBPA. This allows significant amounts of information related to your Exchange configurations to be collected, including SSL configuration, authentication methods, circular logging configurations, and backup status. The Exchange BPA provides different types of scans including a Health Check, Permission Structure Check, Connectivity Test, and Baseline, shown in Figure 17.12.

By default the Best Practice Analyzers updates itself when it starts (this is set by the Check for Updates on Startup option), so as Microsoft identifies new best practices for Exchange you are given the latest information as it becomes available. If your servers are not allowed to connect to the site for updates you will need to manually update the BPA on the systems. As of June 2006 the latest version of BPA auto-updates from http://www.microsoft.com/exchange/code/ExBPA/2.7/en (the URL will change as newer versions become available).

ExBPA Customization Example

The Exchange Best Practices Analyzer Management Pack monitors communication time between the Exchange servers and Active Directory servers in your environment. If Exchange and Active Directory take more than 10 milliseconds to communicate, a warning is generated and you are notified in the MOM Operator console.

The rule used for notification is located at Microsoft Exchange Server Best Practices Analyzer Tool \ ExBPA Event Handling \ ExBPA Warning. If you want to disregard this particular piece of information you would alter the ExBPA Warning rule on the Criteria

tab, Advanced, by adding a condition where the Event Number is not equal to 1192; 1192 being the event number for the 10 millisecond communication test displayed on the alert within the Operator console.

It is recommended to alter this rule rather than disabling it. If the rule is disabled, ExBPA disregards all warnings. The best approach would be to copy the rule, rename it, change the new rule's configuration as discussed previously, and disable the original rule. Disabling a rule prevents a new version of the MP from overlaying it.

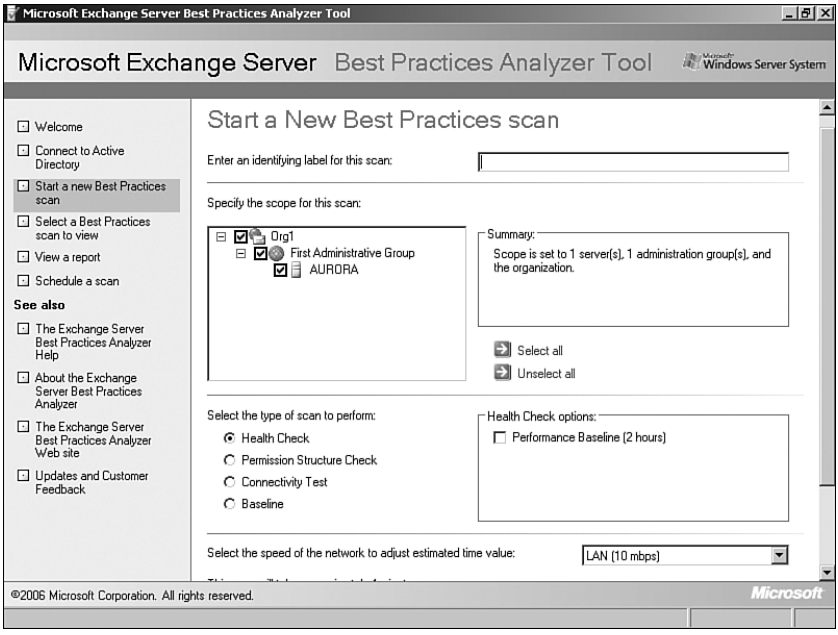


FIGURE 17.12 The Exchange Best Practices Analyzer.

Microsoft Operations Manager 2005 SLA Scorecard for Exchange

The MOM 2005 SLA Scorecard for Exchange is a Solution Accelerator you can use to track service levels of your Exchange servers and identify causes of service outages. The accelerator includes a dashboard that can be used to measure and trend service availability and workloads for your Exchange servers.

There are a number of prerequisites when installing the SLA Scorecard. Most of these will already be implemented if you are using the Exchange MP and MOM Reporting.

- SQL Server 2000 with Service Pack 3 or later
- SQL Server 2000 Reporting Services with Service Pack 1 or higher

- MOM 2005 with the MOM Reporting components installed (Internet Information Services 6.0, .Net Framework version 1.1)
- Exchange 2000 or 2003 Server
- Exchange 2000 and 2003 Management Pack (required for Exchange Internet mail flow measuring)
- Internet Information Services Management Pack
- Antigen Management Pack (tracks antivirus measuring if you use Antigen within your environment)
- Windows 2000 Server or Windows Server 2003 (not Datacenter Edition or implemented on a cluster)
- Office Outlook 2003 or 2000 (to measure client availability) installed on the end-user client
- Internet Explorer 5.0 with Service Pack 2 or above
- MOM 2005 SLA Scorecard for Exchange

The Scorecard for Exchange and SQL Server 2005

The Scorecard was released and tested prior to the release of SQL Server 2005 and Reporting Services 2005. At the time this book was written, Microsoft had not released a compatibility statement for the Scorecard using SQL Server 2005 components in a MOM 2005 SP1 environment.

To install the Scorecard for Exchange when you are already monitoring and reporting on Exchange server, download the SLA, which is available at http://go.microsoft.com/fwlink/?linkid=49639. The zip file you download includes two documents: the MOM 2005 SLA Scorecard for Exchange User Guide and the MOM 2005 SLA Scorecard for Exchange Installation and Configuration Guide.

After downloading and extracting the file, import the SLA .akm (Microsoft SLA Scorecard v1.0 Solution Accelerator.akm) into the management server. Associate the rule groups located under Management Packs \ Rule Groups \ Microsoft SLA Scorecard v1.0 Solution Accelerator with the Microsoft Exchange Installed Computers group and commit your changes. You can then install the Scorecard for Exchange by running the SLAScorecard.msi file.

After the scorecard is installed you need to configure your Exchange servers within the Scorecard for Exchange web interface, which installs by default into http://*<server name>*/slasa. Edit the configuration for your Exchange server(s) by opening the Server Maintenance section of the website. Each of your Exchange servers must be categorized into one of the five available categories (Bridgehead, Internet Gateway, Mailbox, OWA, or Public Folders), and the number of Exchange databases also needs to be specified. For our

example environment there is a single mailbox server named Aurora, which has one database, as shown in Figure 17.13.

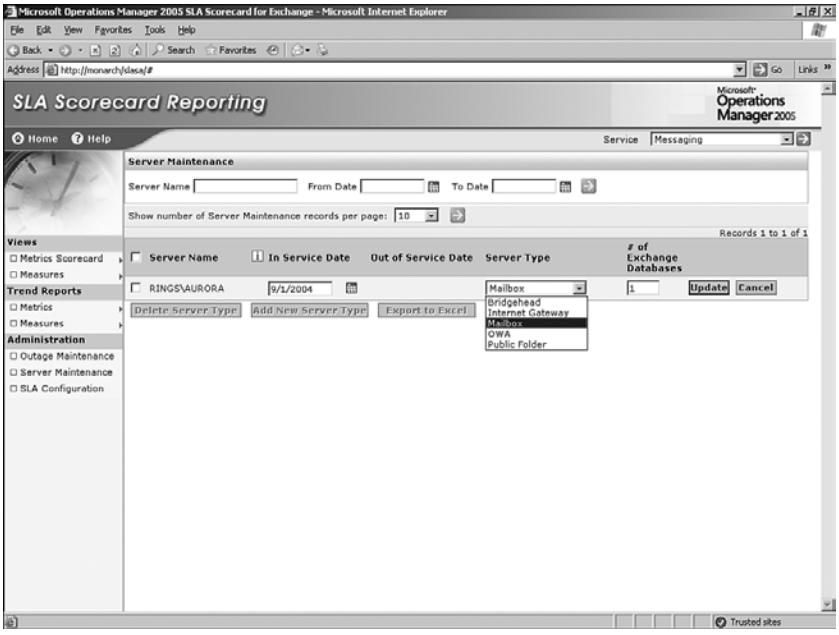


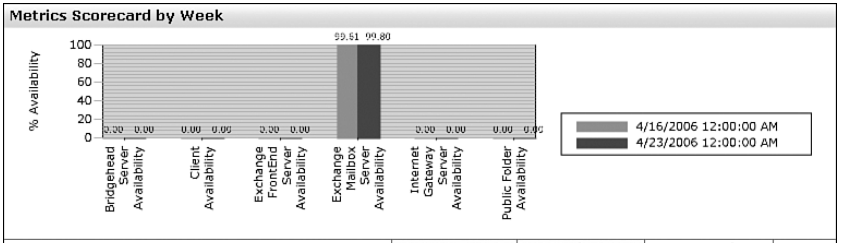
FIGURE 17.13 The Exchange SLA Scorecard Reporting website.

The Scorecard for Exchange provides reports with metrics scorecards (by week or month), metrics trending (by week, by month, or year-to-date [YTD]), and measures trending (by week, by month, or YTD). Figure 17.14 displays the Metrics Scorecard by Week report.

The MOM 2005 SLA Scorecard for Exchange is useful for tracking Exchange server availability and provides information to assist in identifying causes of issues that can result in downtime within your Exchange environment.

Desired Configuration Monitoring Solution Accelerator

The Desired Configuration Monitoring (DCM) Exchange solution accelerator can assist in providing a consistent configuration for your Exchange servers. The solution accelerator uses System Management Server (SMS) 2003 to check for undesired configuration changes. Additional information on this solution accelerator is available at http://www.microsoft.com/technet/prodtechnol/exchange/2003/exsolacc.mspx. The DCM solution accelerator can be integrated with MOM to alert IT staff if configurations are found that are out of compliance.



Metric Name	SLA Target	Last Week - 4/16/2006	Current Week - 4/23/2006	Trend
Bridgehead Server Availability	99.000	0.000	0.000	→
Client Availability	99.000	0.000	0.000	→
Exchange FrontEnd Server Availability	99.000	0.000	0.000	→
Exchange Mailbox Server Availability	99.000	99.614	99.797	↑
Internet Gateway Server Availability	99.000	0.000	0.000	→
Public Folder Availability	99.000	0.000	0.000	→

FIGURE 17.14 Exchange SLA Metrics Scorecard by Week report.

Additional Management Packs to Monitor Messaging

Depending upon how you have designed your messaging environment, there are additional management packs you may want to integrate as part of your monitoring solution.

Microsoft Server Clusters

Microsoft Clustering is often utilized for back-end server configurations, providing a high-availability solution. Clustering in Exchange can be Active/Active or Active/Passive depending on your Exchange design. Clustering can also be extended to larger configurations such as Active/Active/Passive. The Cluster Services Management Pack is available on the Management Pack and Product Connector Catalog website and discussed in Chapter 15, "Managing the Operating System." If your environment is using Microsoft Clustering this management pack makes MOM 2005 fully cluster aware to monitor Active/Passive and Active/Active configurations.

Network Load Balancing

Network Load Balancing (NLB) can be used for Exchange front-end servers to provide a high-availability solution. NLB distributes traffic across a number of hosts giving enhanced scalability and availability of the systems. The Network Load Balancing management pack is also discussed in Chapter 15 and is available at the Management Pack Catalog. If you are using NLB this management pack will detect problems and alert you to critical events within a load-balanced environment.

Exchange Dependencies

Microsoft Exchange is dependent on Active Directory, which in turn is dependent on other services. In Chapter 16, we discussed the components required to manage your Active Directory environment. Your Active Directory infrastructure should be effectively managed and monitored, providing a stable platform for your messaging environment.

Third-Party Tools

We have dedicated significant portions of this chapter to Exchange and the Microsoft management packs available for it. Third-party tools also are available and can assist with managing your messaging environment.

Quest Exchange Reporting

The Quest Exchange Reporting management pack extends the capabilities of MOM 2005 by providing web-based reports that describe usage, financials, capacity, service delivery, and inventory of the Exchange environment. Quest uses an underlying technology called MessageStats, which gathers data from various sources including Exchange tracking logs to provide these reports.

The Quest Reporting management pack provides additional web-based reports for your MOM 2005 environment. An evaluation version of the management pack and additional information on the product is available on its website at www.quest.com.

Antigen

The Antigen products were originally developed by Sybari, an antivirus and anti-spam company recently acquired by Microsoft. The Antigen management pack extends the capabilities of MOM 2005 through integrating events and alerts from Antigen products. The Antigen e-mail and collaboration security products help protect Exchange, the Microsoft SMTP Gateway, Live Communications Server, and Windows SharePoint services from viruses, worms, spam, and inappropriate content. As discussed earlier in the "Microsoft Operations Manager 2005 SLA Scorecard for Exchange" section of this chapter, the Antigen management pack is used with the SLA Scorecard for Exchange Solution Accelerator.

The Antigen management pack extends MOM 2005 to include antivirus and anti-spam management and monitoring. Additional information on the product is available on the Microsoft website at www.microsoft.com/antigen.

Using Third-Party Tools to Manage Messaging

Third-party management packs extend MOM 2005's capabilities to manage your messaging environment. These products can address many challenges in managing messaging.

Reports in the Quest management pack help improve business workflow and configuration of multiple servers. MessageStats provides information that assists in tracking the usage of workflow mailboxes and capacity planning for the Exchange environment.

As with the Exchange management pack, the Antigen management pack can be leveraged to monitor spam within your environment. The Antigen product, until recently a third-party tool, adds antivirus information into MOM 2005. Viruses and spam negatively impact the user's email experience, so removing them assists in providing a better user experience. The Antigen management pack is designed to monitor key services, performance counters, and events needed for an antivirus and anti-spam environment.

Summary

This chapter provided the information required to incorporate management packs to help you monitor and improve your Microsoft Exchange messaging environment. The next chapter discusses using MOM 2005 for database management.

CHAPTER 18

Database Management

IN THIS CHAPTER

- SQL Server Within Your Organization
- SQL Server Management Pack
- Monitoring the MOM Database
- Monitoring the SMS Database
- Other Monitoring Tools

Database administrators (DBAs) wear many hats and perform a wide variety of responsibilities and tasks. In a production environment, a DBA is responsible for the health of databases typically used in high-profile corporate applications. Daily functions generally vary but include a wide variety of tasks such as monitoring space utilization, ensuring that backups are functional, monitoring replication, checking performance, and being cognizant of high activity applications and peak periods of activity.

MOM 2005 can help you with database monitoring by utilizing its SQL Server Management Pack, which includes predefined rules to check the health and availability of Microsoft SQL Server 2000 and 2005.

SQL Server Within Your Organization

The breadth of roles performed by a particular DBA fluctuates from one company to another. A DBA's responsibilities vary based on the size of the organization, whether the firm has centralized its DBA functions, whether database systems administration is managed separately from data administration, and whether any DBA tasks are performed by systems administrators or application developers.

Although Microsoft SQL Server is capable of supporting huge databases and applications, one of its marketing strengths in smaller organizations and departments is the perception that it "just runs itself" because of its automated tuning and maintenance features. In a decentralized IT environment, you may even have individual departments where SQL Server is installed for departmental applications.

SQL Server and Packaged Applications

MOM 2005 also includes the capability in specific management packs to help DBAs with Microsoft system products that use SQL Server as an engine. These capabilities are covered in the "Monitoring the MOM Database" and "Monitoring the SMS Database" sections later in this chapter. MOM can also help you monitor SQL Server when it is implemented with a packaged application and your organization lacks SQL Server-specific expertise. If SQL Server is not your corporate database standard, you might consider investigating whether any third-party management packs are available for MOM 2005 that monitor your particular database technology.

What's Wrong with My Application?

Many issues that hit the help desk and are escalated have the same symptom: poor response time. Poor response time can be caused by a number of things—networking issues, lock contention, online backups, page splits caused by insert or update activity, replication volume, improperly designed databases, or (imagine!) poorly written applications. Although MOM will not rewrite your application or tune your tables, MOM 2005 with the SQL Server Management Pack can help you with monitoring locks, space utilization, backups, and replication.

Tuning Management Packs

Implementing any management pack includes tuning it to meet the requirements of your particular environment. The basics of tuning are covered in Chapter 13, "Administering Management Packs." Specific steps involved in implementing each management pack include utilizing the processes discussed in that chapter.

SQL Server Management Pack

The Microsoft SQL Server Management Pack (MP) includes many functionalities, some of which may be more applicable for your environment than others. You can utilize the SQL Server MP with MOM 2005 to address as few or as many areas of concern as necessary.

Monitoring Management Packs

For purposes of this discussion, we will assume that the management packs discussed are being deployed by MOM administrators working with DBAs to ascertain the particular areas of monitoring important for their environment.

The SQL Server MP helps monitor your application by monitoring database activity. The management pack provides proactive and reactive monitoring of your SQL Server environment. It detects failures and lowers the time required to resolve problems, and presents answers to questions the database administrator may have, such as

- Is the SQL Server available and is it accepting connections?—If users cannot connect to the SQL Server, MOM notifies you of the situation.

- What's the health of my databases? Do all databases and logs have sufficient free space? Are SQL Server transactions being blocked?—Blocking occurs when a transaction locks the resources that another transaction needs to read or modify. Blocking is temporary by its nature but can negatively impact the user's application experience.
- Are SQL Server Agent jobs (backup, optimize, data transformation, and so on) working?—The SQL Server Agent is used to schedule maintenance activities against your databases. If the jobs are not running properly, database maintenance is not taking place as expected.

Setting an Override

If no agent jobs are defined on the specific database server and you do not want to run the SQL Server Agent service, you could set an override to ignore the rules for that database server.

- Is SQL Server replication working?—By default, SQL Server replication monitoring is not fully enabled. If you are using SQL replication in your environment, you will want to monitor replication. We discuss its configuration in the "SQL Server Replication Monitoring" section later in this chapter.

Locate, Download, Install

From the Management Pack Catalog at http://go.microsoft.com/fwlink/?linkid=43970, download the SQL Server 2000, 2005 Management Pack for MOM 2005. Be sure to use a current copy of the management pack (rather than the one on the MOM 2005 installation media) for a version that includes SQL Server 2005 SP1 monitoring support and localization.

Checking the Management Catalog

The management packs shown in the catalog may change as new management packs for new versions of software become available. You can also implement the MP Notifier, discussed in Chapter 13, to notify you when a new version of an implemented management pack is released.

The downloaded extract includes two significant files:

- Microsoft SQL Server MP.akm—The management pack itself
- Microsoft SQL Server MP Reports.xml—Report definitions

After downloading the package, follow the procedures documented in Chapter 13 to extract and install the management pack. Reports are included with the SQL management pack, so if you have already installed MOM Reporting you would choose the Import

Management Packs and Reports option during the import process. Verify that you have deployed agents to your SQL Servers because those systems will need the MOM agent installed to fully utilize the management pack.

Installing Agents

Agents are discussed in detail in Chapter 9, "Installing and Configuring Agents." For SQL Servers in a nontrusted domain or workgroup, you must manually install the MOM agent on the target server. Information is available in Chapter 11, "Securing MOM."

Agentless Monitoring

If you are considering monitoring your SQL Server using the agentless monitoring technique, keep in mind that without using an agent the SQL MP does not support event collection from the SQL Server application log, tasks that start and stop SQL Server Services or SQL Server Agent services, or tasks that start and stop SQL Mail.

The management pack guide for SQL Server is the SQL Server Management Pack Guide, which you can download from the MOM 2005 Product Documentation page at http://i.microsoft.com/mom/techinfo/productdoc/default.mspx. The SQL Server MP guide is also included with the SQL Server package downloaded from the management catalog.

Real World—Tying It All Together

For the database administrators and architects asking: "What MOM will monitor? What instances and databases does it monitor? Does it monitor replicating servers? How about my SQL cluster? Does it support database mirroring? How does that black box work?" here's the answer: By default MOM 2005 monitors all instances and all databases on your servers unless specifically excluded in the SQLExclude.txt file (the model database is not monitored for free space). MOM 2005 supports monitoring for replication, but each replicated server needs to be running the MOM agent. Mirroring support using Windows Management Instrumentation (WMI) is included. And finally, MOM 2005 is fully cluster aware including Active/Passive and Active/Active configurations.

The SQL management pack determines what servers to monitor based on relationships established between computer groups and rule groups. For example, the Microsoft SQL Server 2005 computer group contains all computers running SQL Server 2005, which is determined by a discovery process. One of the rule groups associated with the computer group is the SQL Server 2005 State Monitoring and Service Discovery rule group. This association establishes that all computer systems discovered running SQL Server 2005 will have the rules in the SQL Server 2005 State Monitoring and Service Discovery rule group applied to them.

The discovery process runs every night by default at 2:05 a.m. You can of course initiate computer discovery at any time using the Administrator console, under Administration \ Computers \ Computer Discovery; then right-click and select Run Computer Discovery Now.

Out-of-the-box, no specific steps are required to configure the SQL management pack unless you are using SQL Server replication or client-side monitoring. Based on your particular requirements, you may decide to adjust a number of areas, including changing the free space monitoring thresholds or removing a particular database from monitoring. You may also want to implement the MOM agent with low-level security privileges.

SQL Server Replication Monitoring

SQL Server replication enables you to copy, distribute, and potentially modify data across your enterprise. Replication can be used in a variety of ways, including distributing database processing across multiple servers and separating online transaction processing from decision support systems. Replication implementations can be complex and require significant debugging when data does not show up as expected at the target (subscriber). Depending on how you have configured replication, it can also have a significant impact on your network, which manifests itself as increased response time.

Network impact will vary, based on a number of things including the type of replication, how often you are synchronizing, the type of changes being applied, how many subscribers there are, and so on. You can benchmark the traffic using a utility such as Microsoft's Network Monitor (NetMon), which captures network traffic for display and analysis.

Real World—Replication Tuning

One way to tune replication for better performance is by filtering the data before publishing it. Use the Operator console to check the performance counters for data sent to your Distributor and Subscriber(s) to determine how much data is being sent to those systems. Counters to examine could include

- Replication Merge Downloaded Changes / second
- Replication Snapshot Delivered Trans / second
- Replication Logreader Delivered Trans / second
- Replication Distributor Delivered Trans / second

As discussed in the "Replication Performance Rules" section of this chapter, the replication counters are initially disabled.

Configure Event Rules

The SQL Server MP monitors the health and availability of SQL Server replication and alerts when there are replication failures. The event rules are based on replication events written to the Windows Application event log for that particular server. Using the MOM Administrator console, you may want to review these rules and determine whether you want to toggle the enabled/disabled status of any of the replication event rules.

The location of this particular rule group varies depending on the version of SQL Server you are monitoring:

- If you are using SQL Server 2005, the rules are found at Management Packs \ Rule Groups \ Microsoft SQL Server \ SQL Server 2005 \ Event Collection \ SQL Server Replication \ Event Rules.
- For SQL Server 2000, the rule group is located at Management Packs \ Rule Groups \ Microsoft SQL Server \ SQL Server 2000 \ SQL Server 2000 Event Collection \ SQL Server Replication \ Event Rules.

Replication Performance Rules

Of even greater significance for replication than the event rules are the replication performance collection rules. Because SQL Server replication is not used by every organization running Microsoft SQL Server, the rules are initially disabled in the management pack. If you use SQL replication within your environment and want to monitor replication, you need to enable this performance group using the following procedure:

1. In the Administrator console navigate to Management Packs \ Rule Groups \ Microsoft SQL Server \ Server Performance Collection \ Replication Performance Collection \ Performance Rules. These rules give you a snapshot of how replication is performing in your environment.
2. For each rule listed right-click on the rule and go to the Properties page.
3. On the General tab, check the Enabled check box.
4. The only rules in this rule group are the replication rules in the Performance Rules folder, which are displayed in Figure 18.1.
5. After enabling the rule group, right-click on the Management Pack folder and choose Commit Configuration Change to immediately apply your changes to each of the monitored servers.

Enabling and Disabling Rules

You may also use the MOM 2005 Resource Kit Rule and Group Toggle Utility to enable and disable rules. This utility is described in Chapter 13.

SQL Client Monitoring

Although the database server can appear to be functioning properly, the help desk may receive calls regarding slow response times. The SQL Server Management Pack uses synthetic transactions to assist in troubleshooting response time. These transactions monitor how SQL functions from the client/workstation's side or perspective. The management pack includes computer groups for Client Side Monitoring of SQL Server 2005 and SQL Server 2000. Each computer group includes workstations or servers on the network that monitor SQL Server's functionality and performance for that particular version of SQL Server. The MOM agent must be installed on these systems.

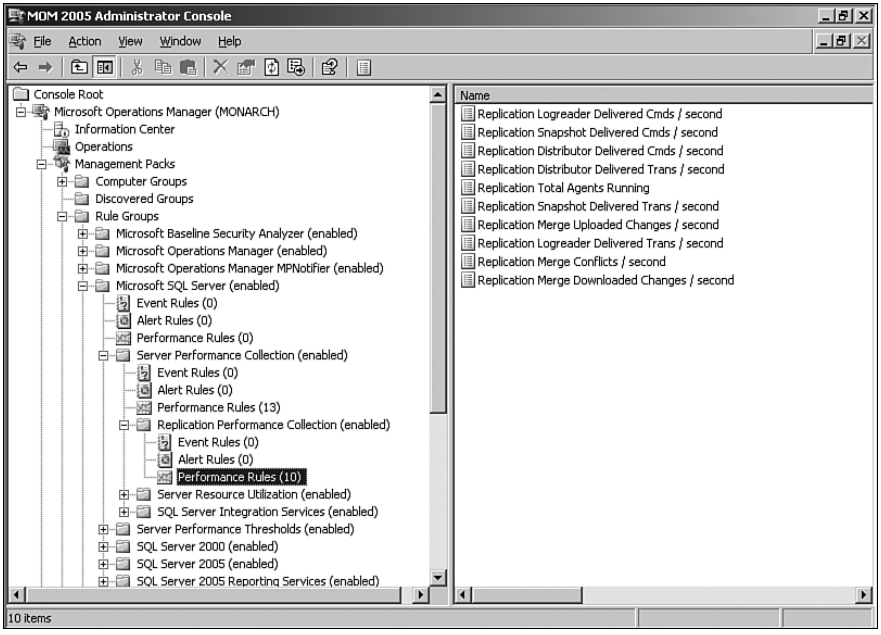


FIGURE 18.1 Replication performance rules.

Client Monitoring Prerequisites

To implement SQL client monitoring, you must first install the appropriate version of client components for your SQL Server installation on the designated client system(s).

Using the SQL Server installation media, navigate to and execute the setup program. The specific screens will vary based on whether you are installing the SQL Server 2005 Workstation Components or the SQL Server 2000 Client tools. If you are installing the SQL 2000 tools, ignore the SQL Server 2000 SP2 and below warning message; after installing the tools apply SQL Server 2000 Service Pack 3a or a later version.

By default the SQL Server Client Side Monitoring groups do not include computers; you must specify the computers to use for Client Side Monitoring. After installing the SQL client components on the target systems, perform the following steps in the MOM Administrator console to add computers to the appropriate SQL Server Client Side Monitoring group:

1. In the Navigation pane at Management Packs \ Computer Groups \ Microsoft SQL Server *<version>* Client Side Monitoring, right-click and select Properties. Click on the Included Computers tab, and Add computers to the group to identify client machines to monitor SQL performance.

2. On the Search for Computers tab you would add in the systems you want to use for SQL Server monitoring. Optionally, you can choose which types of computers to

add from the check boxes, which include Servers, Clients, Domain Controllers, Unknown, and Cluster Virtual Server, as illustrated in Figure 18.2.

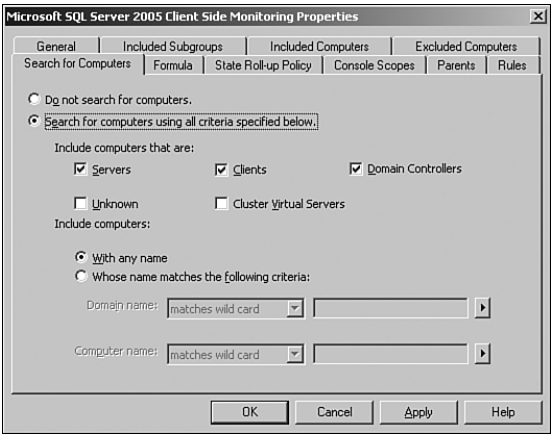


FIGURE 18.2 Client Side Monitoring—Search for Computers tab.

3. When complete, click OK to exit the Microsoft SQL Server *<version>* Client Side Monitoring Properties page.
4. Right-click on Computer Groups and choose Calculate Group Membership. Calculating Group Membership ensures that you see the latest group membership data. All included subgroups and computers, excluded computers, searches, and formulas (including formulas based on membership in discovered groups) are reevaluated.

After you commit your configuration changes, MOM deploys the appropriate rules to the clients that were identified.

The SQL client-side monitoring rules run a script to verify connectivity to the SQL Server databases. These rules provide notification to MOM if there is a failure executing, or a warning if the script took longer than expected to execute. The connectivity script runs every 15 minutes and is configurable in the Administrator console under Management Packs \ Rule Groups \ Microsoft SQL Server \ SQL Server *<version>* \ Client Side Monitoring \ Event Rules \ SQL Server Remote Connectivity. The timing can be set on the Data Provider tab, and the script itself is available on the Responses tab.

How Often to Run the Script?

A question that often arises is: "What is the impact of checking more or less often?" Changing the timing so that the script runs less often will reduce the amount of overhead but also lowers the frequency of checking how often connectivity is verified. Lowering the value will add to the amount of overhead, but you will find out sooner if there is a problem.

You can customize the parameters of the script to specify what instances to check, what database to run the query against, how long the expected execution time will be, whether information events should be generated whenever the script runs, and what specific query runs against the database:

1. Right-click on the SQL Server Connectivity Event rule and select Properties.
2. On the Responses tab edit the SQL Server <*version*> Remote Connectivity script.
3. Change the values of the parameters used in this script in the Launch a Script screen shown in Figure 18.3.

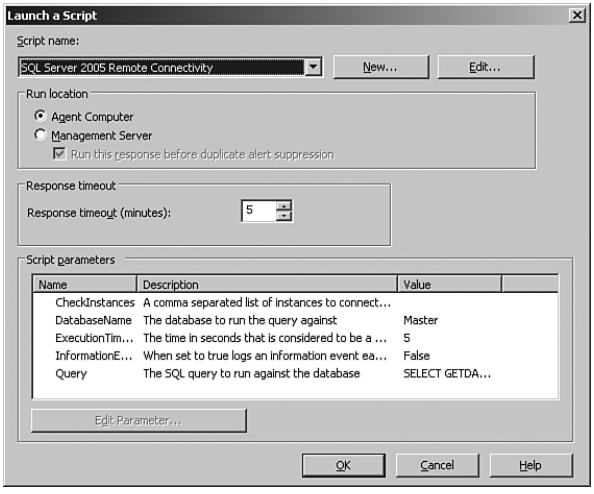


FIGURE 18.3 SQL Client Monitoring script parameter changes.

SQL Server Remote Connectivity Script

The Remote Connectivity script by default runs against the master database, using the `getdate()` function as a basic function that returns the current system date. To monitor in a more granular fashion, you may want to create individual rules for specific instances and check for an important database specific to that instance.

Space Utilization

The SQL Server Management Pack checks free space for databases and transaction logs. You can modify the default thresholds and also exclude specific databases from monitoring.

Configuring Database Thresholds

The management pack monitors the available space on servers running the MOM agent. The free space check runs hourly and by default checks all databases and transaction logs

on each monitored system running SQL Server. The MOM script that assesses free space considers various factors including database automatic growth, multiple file groups, and multiple files. Default thresholds for available free space are defined and can be configured at a granular level.

Customizing Thresholds

You can establish individual thresholds for specific user databases by using overrides or customized scripting. Scripting concepts are discussed in Chapter 22, "Using and Developing Scripts."

The scripting would include adding parameters and new logic to (a copy of) the script for another category of database, a way to indicate those databases, and logic to calculate space.

The rule for monitoring database thresholds is enabled when the management pack is installed. The rule is located at Management Packs \ Rule Groups \ Microsoft SQL Server \ SQL Server *<version>* \ State Monitoring and Service Discovery \ Event Rules.

The name of the rule itself varies based on the version of SQL Server you are monitoring:

- The SQL Server 2005 rule is SQL Server Database Space Analysis.
- The name of the SQL Server 2000 rule is SQL Server Space Analysis.

On the Responses tab, edit the SQL Server *<version>* Space Analysis script to change the parameters used with the rule. The script parameters are listed at the bottom of the screen; clicking the Edit Parameter button displays the screen shown in Figure 18.4.

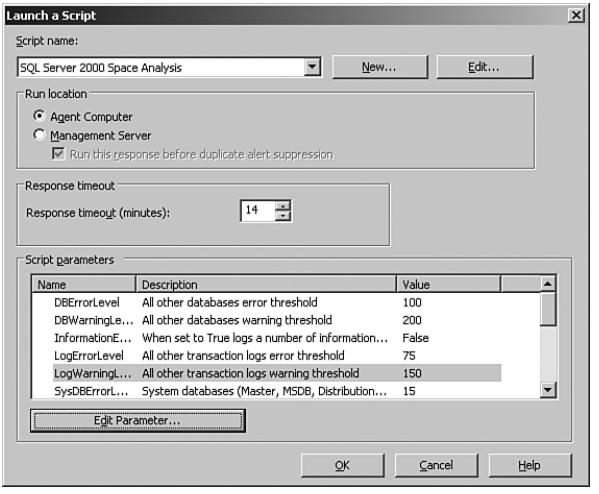


FIGURE 18.4 SQL free space threshold parameter changes.

After modifying any scripts, commit the configuration changes to immediately update them on your monitored systems. This process was discussed in Chapter 13.

If you are changing the default threshold free space configuration you should discuss what these values should be with any DBAs who will be impacted by the change. SQL Server 2000 free space thresholds are measured in megabytes only, whereas the SQL Server 2005 rule measures thresholds as a percent—using a default of 20% freespace as a warning threshold and 10% remaining freespace an error.

Table 18.1 lists the default threshold configurations for free space monitoring on SQL Server 2000 databases.

TABLE 18.1 Default SQL Free Space Thresholds for SQL Server 2000 Databases

Database	Warning Threshold	Error Threshold
General Databases	200MB	100MB
General Transaction logs	150MB	75MB
System Databases (msdb and master)	30MB	15MB
System Transaction Logs (msdb and master)	30MB	15MB
Tempdb	150MB	75MB
Tempdb Transaction Logs	200MB	100MB

The General database type applies to all databases except for those listed in Table 18.1. The Model database is not monitored for free space. Any databases set to autogrow do not generate free space warnings or errors.

Monitoring Free Space

The SQL Server MP includes public views to help monitor disk space, which are found in the Operator console at All Public Views \ Microsoft SQL Server \ SQL Server *<version>* \ Server Resource Utilization \ Disk Capacity. Free space is measured as both a percent and in megabytes. These views can be used to help monitor systems where databases are set to autogrow.

Removing a Database from Monitoring

Individual databases can be excluded from MOM 2005 monitoring by including their names in an exclusion file. The exclusion file is simply a text file on the database server being monitored. The file needs to be saved on the root of the C: drive as c:\SQLExclude.txt. The content of the file includes a list of database names, one per line. If multiple instances are active on the SQL Server, the instance name precedes the database name. If an instance is not specified, it is assumed to be the default instance.

The following is an example of an exclusion file:

```
Northwind
Master
Pubs
```

```
Instance1\Northwind
Instance1\Pubs
Instance2\Pubs
```

The file should be saved as SQLExclude.txt and placed in the root of the C: drive on the monitored database servers.

Performance

The SQL management pack monitors a number of SQL Server performance metrics. Some of the specific items being monitored include

- Memory Grants Pending
- Page Writes / second
- Lock Blocks
- Log Cache Reads / second
- Log Truncations
- Mixed Page Allocations / second
- Logins / second
- Active Transactions
- DBCC Logical Scan Bytes / second
- Full Scans / second
- Lock Timeouts / second
- Average Wait Time (ms)
- Pages Allocated / second
- Percentage of CPU used by SQL Server processes such as SQLAGENT, SQLSERVR, SQLBROWSER, and SQLMANGR

These counters are checked every 15 minutes by default using the Windows performance counters. (To modify how often MOM checks the counters, modify the data provider for each counter and change the sample time.) There are also multiple replication performance counters you may want to examine under Management Packs \ Rule Groups \ Microsoft SQL Server \ Server Performance Collection. The SQL management pack also provides default threshold levels for performance metrics for the following rules, listed in Table 18.2.

TABLE 18.2 SQL Performance Threshold Rules

Rule Name	Default State
Cache Hit Ratio < 90% for 15 minutes	Enabled
SQLSERVR Process > 90% CPU for 15 minutes	Disabled
SQLAGENT Process > 90% CPU for 15 minutes	Disabled
Access Methods : Full Scans > 2 for 15 minutes	Disabled
Buffer Manager : Page Life Expectancy < 300 second	Disabled
Locks: Number of deadlocks > 1 for 15 minutes	Enabled
SQL Server User Connections > 500	Enabled

These rules can be enabled or disabled depending on your specific requirements, and you can also change the thresholds for each of these rules. For example, you can set the number of SQL Server User Connections in this rule group from 500 to whatever value is more appropriate for your organization. To change the value, browse to Management Packs \ Rule Groups \ Microsoft SQL Server \ Server Performance Thresholds \ Performance Rules. Right-click on the SQL Server User Connections > 500 Performance rule and select Properties. On the Threshold tab shown in Figure 18.5, set the Greater Than the Following Value to a new value.

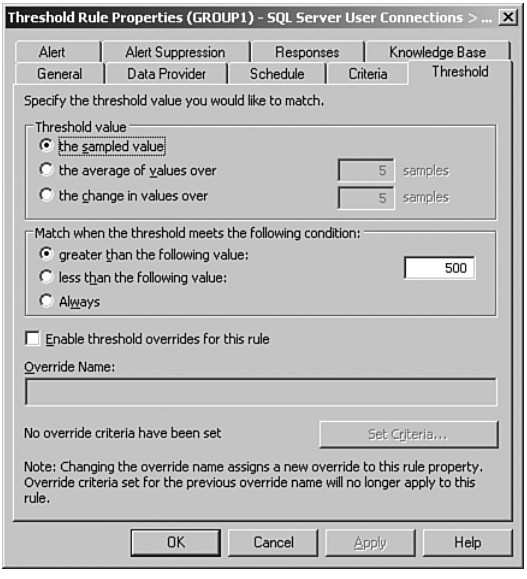


FIGURE 18.5 Changing the threshold for User Connections.

Monitoring System Resources

For high-volume and high-availability database servers, you may want to also monitor system resources and performance including the balance between CPU, memory, and disk access. The Windows System Resource Manager MP can also be utilized for Windows Server 2003 Enterprise and Datacenter editions. System monitoring is discussed in Chapter 15, "Managing the Operating System."

This particular rule is also a good candidate for a threshold override. You could override the value to be higher or lower, depending on the particular server. The steps to create the threshold are

1. From the Properties page for the SQL Server User Connections > 500 Performance rule, again select the Threshold tab, and check Enable Threshold Overrides for This Rule.
2. Specify a meaningful name for this threshold, such as Fountain_User_Connections_Override_Threshold.
3. Select Set Criteria and add your Override Target Computer Group or Computer (Fountain in our case).
4. Specify a Value as shown in Figure 18.6 and click OK.

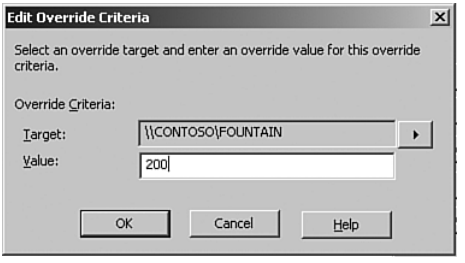


FIGURE 18.6 Overriding the threshold for a particular server.

Monitoring Database Mirroring

SQL Server 2005 SP1 and later versions of SQL Server support database mirroring. Database mirroring continuously transfers a database's transaction log records from one SQL Server database (the *principal* server) to a database on another SQL Server, the *mirror* server. The mirrored copy is a standby copy and is used only in a failover situation. An optional component is the *witness*, another instance of SQL Server that acts as an intermediary between the principal and the mirror, determining when to failover. The witness server is only used when you want to implement automated failover.

Database mirroring does not support log records from bulk-logged operations, and the principal database must use the Full recovery model. Information on SQL Server 2005

mirroring is available at http://www.microsoft.com/technet/prodtechnol/sql/2005/dbmirror.mspx.

The SQL Server MP includes rules to monitor database mirroring, located at Management Packs \ Microsoft SQL Server 2005 \ Database Mirroring Monitoring. A child rule group, Database Mirroring Monitoring Event handlers, monitors overall mirroring health. Rules check the status of the witness and connections between the principal and mirror hosts. There is also a Database Mirroring Query – Default Instance group. This child rule group contains an event rule that uses WMI to monitor database mirroring for the default database instance. You can modify the management pack to monitor a named instance by performing the following steps:

1. Create a new rule group for the instance, similar to the Database Mirroring Query – Default Instance rule group, with a single event rule that adds a WMI provider. The WMI provider has a namespace of root\Microsoft\SqlServer\ServerEvents\<*instancename*>. Specify the following query in the WMI provider:

```
Query SELECT * FROM DATABASE_MIRRORING_STATE_CHANGE
Property List StartTime, ComputerName, SQLInstance, DatabaseName, DatabaseID,
State, TextData
Response
```

2. Create a computer group as a member of the Microsoft SQL Server Mirroring Discovered Group <*instancename*>.
3. Add the rule group to the computer group.

Excluding Agent Jobs from Long-Running Agent Job Monitoring

The SQL MP monitors all jobs that run on a SQL Server to determine whether they complete in a specific amount of time. If the jobs run too long a warning or error is sent to MOM to notify regarding the status of the job. You can change the monitoring for the particular version of SQL Server you are monitoring:

- The SQL Server 2005 rule is located in the Administrator console at Management Packs \ Rule Groups \ Microsoft SQL Server \ SQL Server 2005 \ State Monitoring and Service Discovery \ Event Rules \ SQL Server Agent Long Running Jobs.
- For SQL Server 2000, navigate to Management Packs \ Rule Groups \ Microsoft SQL Server \ SQL Server 2000 \ SQL Server Health and Availability Monitoring \ Event Rules \ SQL Server 2000 Long Running Agent Jobs.

Open the rule, and on the Responses tab, edit the SQL Server <*version*> Long Running Agent Jobs script. The following script parameters are available:

- WarningThresholdInMinutes—This value is set to 60 by default. This value determines how many minutes SQL Server Agent Job can run before it generates a warning alert.

- ErrorThresholdInMinutes—The default value is 120. This value determines how many minutes SQL Server Agent Job can run before it generates an error alert.
- InformationEvent—This configuration is set to False. If changed to True an information event is logged each time the script runs. Information events can be used to assist in troubleshooting.

If you change any of the preceding script parameters, it applies to all scripts that are run. There may be situations where you have specific agent jobs that will run longer than your normal thresholds for warnings and events; for this situation create a text file of the agent jobs to exclude from monitoring as long running agent jobs. The text file needs to be saved on the root of the C:\ drive as c:\SQLMPAgentExclude.txt. The contents of the file have the following format:

- List the `agentjobname`, one per line in the field. The job name is the name of the job as it appears in the sysjobs table in the msdb database.
- If multiple instances are active on the SQL server, the instance name precedes the database name, for example: instance1\job1. If an instance is not specified, it is assumed to be the default instance.

Sample entry for a default instance follows:

```
agentjobname
```

Sample entry for a named instance follows:

```
instancename\agentjobname
```

Save the file as SQLMPAgentExclude.txt and place it in C:\ on the monitored servers.

Monitoring Multiple Thresholds

To specify different monitoring thresholds for excluded jobs you would need to create a custom rule or use overrides.

Real World—Monitoring Long-Running Jobs

A slightly different scenario may arise when you have long-running jobs that you want to exclude from Agent Job Monitoring, yet are still interested in the status of those jobs. You may want to monitor when a specific job finishes.

You could approach this by having the job write an event with a unique event ID to the application log as it completes. You could monitor for the event in one of several ways:

- Create an event rule (Alert or Respond to Event) in MOM to detect that specific event ID and generate a Success or Information alert.
- Create an event rule of type Detect Missing Event if the job does not complete, generating a Warning or Error alert. This would just tell you whether the job had finished by a particular time, not when it actually finished.

Configuring the Agent for a Low-Privilege Scenario

Monitoring functionality on an agent computer is provided by both the MOM Service process (MOMService.exe) and the Agent action account. Whereas on Windows 2000 the Action account must be a member of the local Administrators group, Windows 2003 systems have the capability to use a low-privileged account for the Action account. However, defining the necessary rights and privileges for the Action account to run the SQL Server Management Pack requires significant manual configuration. For Windows Server 2003 systems, the Action account must have the following privileges:

- Member of the Local Users group
- Member of the Performance Monitor Users group
- Manage auditing and security log user right
- Allow log on locally user right

Checking the Management Packs Assigned to an Agent

You can run a SQL query to determine which computer groups a particular computer belongs to and use that information to determine which management packs will be deployed to the agent. A sample query, using the MOM 2005 SDK SDKComputerToComputerGroupView is

```
select ComputerGroupName, ComputerName from SDKComputerToComputerGroupView
where ComputerName = 'monarch'
```

This query checks the Monarch server for computer group membership.

To function in a low-privileged scenario, the SQL Server Management Pack requires that the account used for the Action account and the service context that the MOM service runs under have additional rights and privileges, which are listed in Table 18.3.

TABLE 18.3 Access Types Required for the Action Account

Resource	Access Type	Instructions
Windows Event Log	Read	Give the Action account the "Manage auditing and security log" privilege by setting Local or Group policy.
SQL Server Registry Keys	Read	Add the Action account to the registry properties of HKLM\SOFTWARE\Microsoft\Microsoft SQL Server, providing Read access. Also add the Action account to the registry properties for each named instance underneath this registry key with Read access.

TABLE 18.3 Continued

Resource	Access Type	Instructions
		For the default instance, add the Action account and provide Read access to the following registry key and the subkeys listed here: HKLM\SOFTWARE\Microsoft\MSSQLServer: Setup MSSQLServer MSSQLServer\Parameters Replication Manually configure these subkeys; the default instance does not pass permissions to lower keys.
Security login rights to each instance	Grant access	For each instance on a managed SQL Server computer, give the Action account Grant access rights for security logins.
Access to the master database for each instance (required to monitor long-running agent jobs)	Permit	For each instance on a managed SQL Server computer, give the Action account Permit access to the master database. In SQL Server Management Studio, add the Action account to the *<instancename>*\Databases\Master\Security\Users node. (In SQL Server Enterprise Manager, add the Action account to the *<instancename>*\Databases\Master\Users node.) Keep the default permissions associated with this new user.
Access to the sysjobs table of the msdb database for each instance (required to monitor long-running agent jobs)	Select	For each instance on a managed SQL Server computer, give the Action account Select permissions to the sysjobs table of the msdb database. In SQL Server Management Studio / SQL Server Enterprise Manager, this table is located in the following node: *<instancename>*\Databases\msdb\tables\(system tables)\sysjobs. Open the properties for the table, click Permissions, and check SELECT for the Action account.
Permissions to the `xp_sqlagent_enum_jobs` extended stored procedure for each instance (required to monitor long-running agent jobs)	Execute	For each instance on a managed SQL Server computer, give the Action account Execute permissions to the `xp_sqlagent_enum_jobs` extended stored procedure. In SQL Server Management Studio / SQL Enterprise Manager, this procedure is found at the *<instancename>*\Databases\Master\ (Programmability)\Extended Stored Procedures node. Open the properties for the procedure, click Permissions, and check EXEC for the Action account.

TABLE 18.3 Continued

Resource	Access Type	Instructions
Permissions to the SQL Server 2000 `xp_startmail` and `xp_stopmail` extended stored procedure for each instance (required to run the Stop and Start SQL Server Mail tasks)	Execute	For each instance on a managed SQL Server 2000 computer, give the Action account execute permissions to the `xp_startmail` and `xp_stopmail` extended stored procedures. Open the properties for each of these procedures, click Permissions, and check EXEC for the Action account.
Access to the database (required to run the SQL Server Service Discovery script)	Default access	For each database, add the Action account to the list of users. Db_owner role membership is not required to run the SQL Server Service Discovery Script, although db_owner membership is required to run the SQL Server Space Analysis script, as noted in the following item in this table. In SQL Server Management Studio / SQL Enterprise Manager, navigate to Databases \ <*database*> \ (Security) \ Users and add the Action account.
Db_Owner access to the database (required to run the SQL Server Space Analysis script)	Db_Owner	For each database, add the Action account to the list of users with the db_owner role membership. In SQL Server Management Studio / SQL Enterprise Manager, navigate to Databases\ <*database*> \ (Security) \ Users. Add the Action account and assign the db_owner database role membership.
SQL Server Resource Files	Read and Execute	For each instance on a managed SQL Server computer, the service account (Network Service) that the MOM service is running under must have access to the following resource files: SQLEVN70.rll SQLAGENT.dll In the Security properties for these files, add the Network Service service account and give the account both Read and Execute permissions.

After granting these privileges, use the SetActionAccount utility to configure the account as the Agent Action account. This utility is documented in Chapter 11. You would then use the MOM Administrator console to update the Agent settings by right-clicking on the computer under Administration \ Computers \ Agent-managed Computers and selecting Update Agent Settings.

Restricted Tasks with a Low-Privileged Action Account

If you use a low-privilege account, a number of management pack tasks are not supported:

- Start SQL Service
- Stop SQL Service
- Start SQL Agent
- Stop SQL Agent

These tasks will not function properly in the Operator console.

Implementation Tips

As part of your management pack implementation, there are a number of performance counters that you may want to examine and enable/disable depending on your particular environment. You also want to ensure that you are capturing the data you need for reports.

Health and Availability

The SQL management pack checks for database health, service availability, replication monitoring, and free space analysis as was discussed in the "Configuring Database Thresholds" section earlier in this chapter. Another area of customization is specifying which databases are considered to be high-severity databases, meaning that these are critical databases within your environment. If a database is defined as a high-severity database, the management pack generates a Service Unavailable alert if the database is unavailable.

By default, the list of high-severity databases includes master, tempdb, model, and msdb. SQL Server 2000 also considers the distribution and OnePoint databases as high severity. These names can be changed in the Administrator console under Management Packs \ Rule Groups \ Microsoft SQL Server \ SQL Server <*version*> \ State Monitoring and Service Discovery \ Event Rules \ SQL Server Database Health. On the Responses tab edit the SQL Server Database Health script, and under the Script Parameters you can edit the HighSevDatabases value parameter as shown in Figure 18.7.

Security Reports

Several security reports provided with the SQL management pack are not automatically populated with data. The following reports will not function unless specific monitoring rules are enabled in the SQL management pack. These rules are disabled by default to reduce agent communication traffic in MOM environments not using MOM reporting:

- All Failed Logins by Count
- Top 25 Percent Failed Logins
- All Successful Logins by Count
- Top 25 Percent Successful Logins

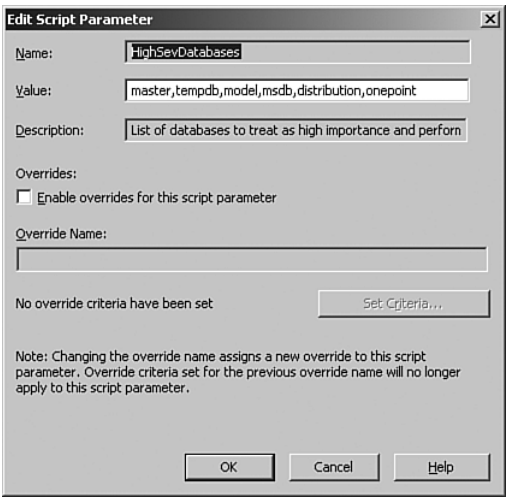


FIGURE 18.7 Altering the HighSevDatabases value.

The location of the event rules discussed in Table 18.4 varies based on the version of SQL Server you are monitoring:

- For SQL Server 2005, navigate to Management Packs \ Rule Groups \ Microsoft SQL Server \ SQL Server 2005 \ SQL Server Report Collection Rules.
- The SQL 2000 rules are located at Management Packs \ Rule Groups \ Microsoft SQL Server \ SQL Server 2000 \ SQL Server 2000 Report Collection Rules.

Table 18.4 describes the configuration requirements for these reports:

TABLE 18.4 Report Configuration Requirements

Report	Enable the Following Rules
All Failed Logins by Count	Enable SQL Server auditing (All or Failed) Report Collection - SQL Server <*version*> Failed Logins Report Collection - SQL Server <*version*> Failed Logins (SQL)
Top 25 Percent Failed Logins	Enable SQL Server auditing (All or Failed) Report Collection - SQL Server <*version*> Failed Logins Report Collection - SQL Server <*version*> Failed Logins (SQL)
All Successful Logins by Count	SQL Server auditing (Successful or All) Report Collection - SQL Server <*version*> Successful Logins (Trusted) Report Collection - SQL Server <*version*> Successful Logins (Non-trusted)
Top 25 Percent Successful Logins	SQL Server auditing (Successful or All) Report Collection - SQL Server <*version*> Successful Logins (Trusted) Report Collection - SQL Server <*version*> Successful Logins (Non-trusted)

To locate a particular rule, you can use the Find Rules capability in the Administrator console:

1. In the Navigation pane under Management Packs, right-click on the Rule Groups folder and select the Find Rules option.
2. Specify the Rule Group you want to search (in this case Microsoft SQL Server).
3. Proceed to the Rule Search - General screen shown in Figure 18.8 where you would select to search by Rule Name, contains substring, and the name of the rule you are searching for.

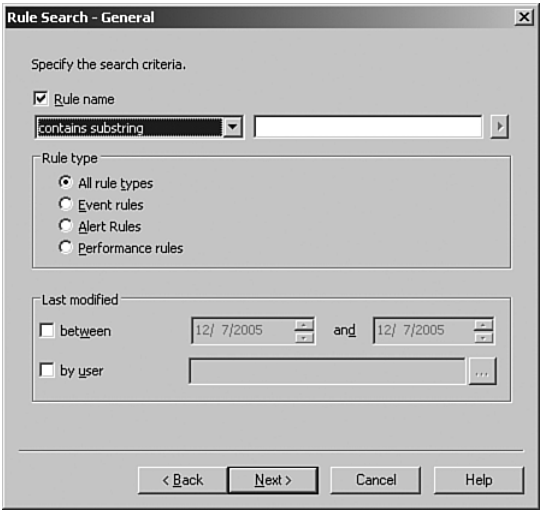


FIGURE 18.8 Searching for a rule in the Administrator console.

Enabling SQL Server auditing

To enable SQL Server auditing, log in to the database server and open the SQL Server Management Studio (SQL Server 2005) or SQL Enterprise Manager (SQL Server 2000) tool. Select the appropriate SQL Server, right-click and choose Properties, and select the Security option.

Select Success to collect data for successful login reports, select Failure to collect data for failed login attempts, or select All to collect both. Recycle the SQL Server for the changes to go into effect.

Auditing SQL Logons

Enabling SQL Server auditing captures information regarding failed and (optionally) successful logon attempts to the Windows Application log. This information can be useful for security purposes. However, SQL Server auditing is enabled at the instance

level, which gives it limited granularlity, and you are limited here to specifying audit levels of None, Failed logins, Successful Logins, or Both (each progressively capturing more data). If you modify your auditing settings, remember to stop and restart the SQL Server service to enable your changes.

Detailed auditing of user actions to an audit log is separately enabled by configuring SQL Server for C2 audit mode. Specifying Server-Side Traces captures an even more granular level of auditing. There is a caveat: the more auditing, the more overhead on your system—which can degrade performance.

Tasks

The SQL Server MP adds a number of tasks to the Operator console, listed in Table 18.5. Note that some support multiple instances.

TABLE 18.5 SQL Server Tasks

Task	Instance-Aware
Display global configuration settings (`sp_configure`)	Yes
Run SQL Server Query Analyzer (SQL Server 2000)	Default instance only
Start SQL Mail (SQL Server 2000)	Yes
Stop SQL Mail (SQL Server 2000)	Yes
Run SQL Server Profiler	Default instance only
Start SQL Server	Yes
Stop SQL Server	Yes
Start SQL Server Agent	Yes
Stop SQL Server Agent	Yes
SQL Server Replication Monitor (SQL Server 2005)	Yes
SQL Server Configuration Manager (SQL Server 2005)	Yes
SQL Server Management Studio (SQL Server 2005)	Default instance only

Configuring SQL Tasks

The SQL Server Profiler, SQL Server Management Studio, Replication Monitor, and Query Analyzer tasks require that the corresponding SQL Server tools be installed on the computer running the MOM Operator console.

Real World—Issues with SQL Server MP Scripts

Several people have noted problems in executing some of the scripts included with the SQL Server MP. These scripts can step on each other, resulting in contention and potential script failures, which then generate alerts. There are four scripts to be concerned with:

- SQL Server Block Analysis—Runs every 5 minutes, synchronized at 00:03
- SQL Server Service Availability—Runs every 5 minutes, synchronized at 00:02

- SQL Server Space Analysis—Runs every 15 minutes, synchronized at 00:12
- SQL Server Service Discovery—Runs every 8 hours, synchronized at 00:20

The SQL Server Service Availability script's execution will overlap that of the SQL Server Block Analysis script any time it runs longer than 1 minute. The best way to resolve this is by changing the frequency of execution and adjusting the synchronization time. For example, you could run the Block Analysis script every 10 minutes synchronized at 00:06, and the Availability script every 10 minutes synchronized at 00:01. As you adjust the scheduling for these first two scripts, ensure that the timing does not conflict with the Space Analysis and Service Discovery scripts.

Additional information regarding these scripts can be found at Pete Zerger's blog (http://www.it-jedi.net/2006/04/sql-server-management-pack-script.html) and John Hahn's blog at http://learnsystemsmanagement.com/community/blogs/mom_2005_blog/archive/2006/04/13/11.aspx.

These scripts are found in the rule groups for both SQL Server 2000 and SQL Server 2005.

Reporting

If MOM Reporting is installed, the SQL MP includes a number of reports. Figure 18.9 shows a sample of the SQL Server Configuration report.

SQL Server Configuration

Microsoft Operations Manager 2005

Description 6/25/2005 3:36:08 PM

Server: CONTOSO\FOUNTAIN
SQL Instance: MSSQLSERVER

SQL Server Property	Value
Version	8.00.194
Service Pack Level	8.00.761
Language	1033
Authentication Mode	Windows Authentication Mode
Clustered	False
Master Database Location	C:\Program Files\Microsoft SQL Server\MSSQL\data\master.mdf
Master Database Log Location	C:\Program Files\Microsoft SQL Server\MSSQL\data\mastlog.ldf
Error Log Location	C:\Program Files\Microsoft SQL Server\MSSQL\log\ERRORLOG
Audit Level	None
Enable Error Reporting	False
Replication Installed	True
Replication Working Directory	C:\Program Files\Microsoft SQL Server\MSSQL\REPLDATA
Replication Distribution Database	N/A

Databases	DB Size(MB)	Autogrow(DB)	DB Log Size (MB)	Autogrow (LOG)	Recovery Model
model	1	True	0.50	True	FULL
pubs	2	True	0.75	True	SIMPLE
wss1	2	True	0.75	True	FULL
SPS01_Config_db	2	True	0.75	True	FULL
contoso1_PROF	2	True	0.75	True	SIMPLE
contoso1_SERV	3	True	0.75	True	SIMPLE
Northwind	4	True	1.00	True	SIMPLE
ReportServerTempDB	5	True	1.25	True	SIMPLE
STS_Snowmass_1	7	True	1.00	True	FULL
contoso1_SITE	9	True	1.00	True	FULL
msdb	16	True	2.25	True	SIMPLE

All dates and times shown in Central Standard Time Page 1/2

FIGURE 18.9 SQL Server Configuration for the Fountain database server.

The User Connections by Day report summarizes over time the number of user connections. This report is illustrated in Figure 18.10.

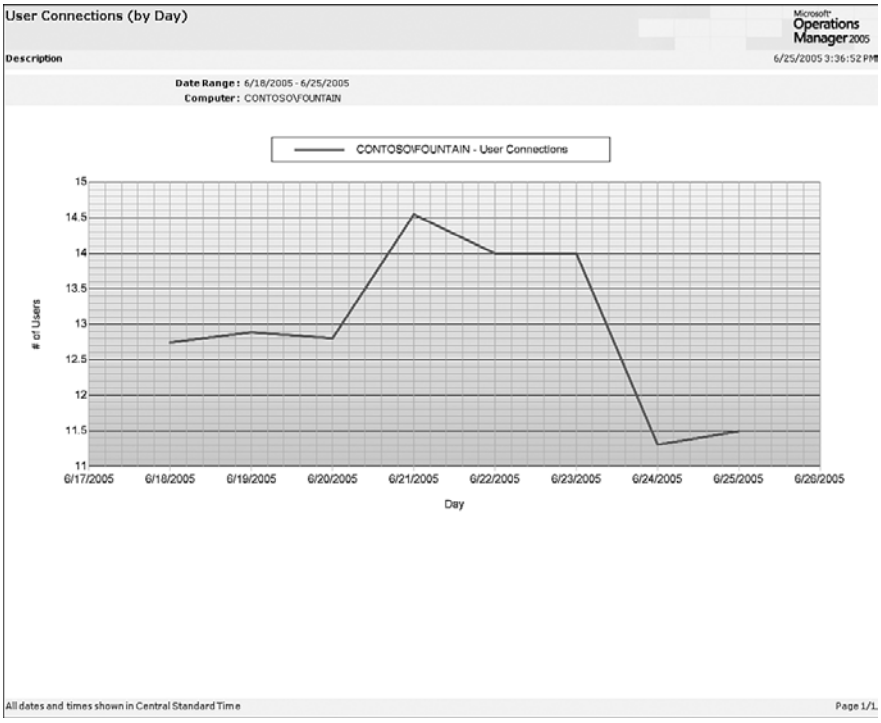


FIGURE 18.10 User Connections by Day for the Fountain database server.

Monitoring SQL Server in a Workgroup

In a decentralized IT environment SQL Server may be installed as part of a workgroup application. For MOM 2005 to monitor SQL Server with this configuration, you would first install the MOM agent on the SQL Server computer using the procedure described in Chapter 11.

You will need to designate a local user account as the Agent Action account. If the server is running Windows 2000, the Action account must be a member of the local Administrators group. On Windows 2003, you can choose to use a low-privileged account, which must be configured as described in the "Configuring the Agent for a Low-Privilege Scenario" section earlier in this chapter. Specify the local account you designated with the SetActionAccount utility using the format COMPUTERNAME\ACCOUNT.

Monitoring the MOM Database

In addition to using the SQL Server 2000 Management Pack to monitor your production databases, the MOM 2005 Management Pack performs a number of functions to verify

that the OnePoint SQL Server database that stores the operational data used by MOM is performing properly. The MOM 2005 MP includes the following functionality:

- Determines whether there are communication problems between the management server and the MOM database server.
- Watches the MOM 2005 database server to validate its functionality. It also checks the OnePoint database to verify that it is not set to autogrow and that SQL Authentication is set to Windows Only.
- Monitors the MOM database server to validate that operational data reports are being sent to Microsoft (if selected as part of your installation process) and that SQL Server Reporting Services is functional.
- Notifies you if the MOM data warehouse SQL Server Agent job fails or the reporting database grooming job fails.
- Provides notification if the Data Transformation Services (DTS) job, which archives data from the OnePoint database to the reporting database, fails.

Although there is no rule to check the MOM database specifically for freespace, Microsoft provides a stored procedure, `sp_onepointfreespace`, loaded with the OnePoint database. The procedure returns the freespace as a percentage. Sample output is as follows:

```
OnePoint Free Data Space Percentage: 84.754
```

On the CD

We have developed a small management pack that tracks and reports on database size and growth statistics for the MOM Operational and Reporting databases.

This management pack creates performance counters that track database size for the OnePoint and SystemCenterReporting databases. The information is used to generate reports that can be used to track current database utilization and project future utilization.

The MOM database tracking executable is a self-extracting zip file including the management pack with reports, database scripts, installation instructions, and documentation. MOMDatabaseTracking.exe is on the CD included with this book.

SQL Authentication Check

If you have a business requirement to use "mixed mode" authentication in your environment, you may want to turn off the alert generated when SQL Server is configured to use SQL and Windows Authentication. In the Administrator console, navigate to Management Packs \ Microsoft Operations Manager \ Operations Manager 2005 \ Database \ Event Rules \ MOM Database State Monitoring. Open the rule and on the Responses tab, edit the MOM Database State Monitoring script. Edit the SQLAuthenticationCheck parameter and enable overrides for the script parameter. Set criteria adding a target computer as shown in Figure 18.11.

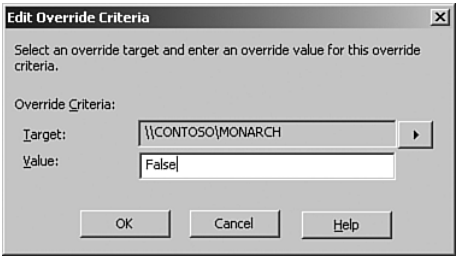


FIGURE 18.11 Override the SQLAuthenticationCheck script parameter.

MOM uses the SQLAuthenticationCheck parameter as a security check for your MOM 2005 environment; using mixed mode authentication will not impact MOM's capabilities.

The MOM 2005 Management Pack is required for MOM 2005 and is automatically installed with the management group. Microsoft Product and Support Services (PSS) will not support a MOM 2005 installation without the MOM 2005 Management Pack installed.

Monitoring the SMS Database

Microsoft's Systems Management Server (SMS) uses SQL Server as its database engine. SQL Server is installed on SMS central and primary site servers. The SMS Management Pack includes functionality to verify the health of SQL Server databases in your SMS environment, including

- Alerting when the SQL Server service, a critical dependent service for SMS, stops or fails to start on SMS site systems
- State monitoring of the site database
- Notifying you if the total number of SQL Server user connections exceeds a threshold on SMS site database servers

Many of the database-related rules in the SMS MP are not initially turned on because similar functionality is provided with the SQL Server Management Pack. However, if you use SQL Server only with SMS, you may want to enable these rules and not implement the SQL Server MP.

Reviewing the SMS Management Pack

Be sure to review disabled rules in the SMS Management Pack to identify those you might want to enable in your environment. A number of rules under Management Packs \ Microsoft Systems Management Server (SMS) 2003 \ SMS Servers \ SMS Site Database Servers are initially disabled.

SMS monitors the basic health of its site systems periodically through its site system status summarizer, which polls SMS site systems once every hour, on the hour. Site system status monitoring provides the ability to monitor and generate an alert when a condition critical to the health of the SMS site system is detected. Some of the monitored status messages include an SMS site system being down, a server running SQL Server that is running with less than 5% available database space or log space, and SMS site systems running out of physical disk space.

Checking Space Utilization

Review the space utilization of the SMS Site SQL Server database and log on a weekly basis.

Other Monitoring Tools

Although MOM monitors the health and availability of your SQL Server environment, a number of other tools are available that complement or extend MOM. You can get a list of current tools interacting with MOM from the Management Pack Catalog at http://go.microsoft.com/fwlink/?linkid=43970. New products are added to the management catalog on a regular basis.

Of course utilities are provided with SQL Server that the SQL Server DBA will use for a variety of other activities to determine what is occurring during daily database operations, as well as numerous third-party tools that do not interact with MOM.

Summary

This chapter provides an arsenal of tools for managing SQL Server. In the next chapter we discuss extending MOM by using product connectors, implementing third-party management packs, and developing your own management packs.

PART VI

Moving Beyond MOM 2005

IN THIS PART

This page intentionally left blank

CHAPTER 19

Interoperability

IN THIS CHAPTER

- Talking to the Rest of the World
- Solution Accelerators

This book has discussed a variety of ways that Microsoft Operations Manager (MOM) provides solutions to various business challenges. One business challenge is effectively monitoring and managing disparate computing and network systems. MOM 2005 uses management packs, connectors, and solution accelerators as tools to enhance its capabilities in managing dissimilar systems. This chapter discusses three themes: using the MOM Connector Framework to connect MOM to other management systems including other MOM 2005 management groups, using various third-party management pack solutions, and using Microsoft's solution accelerators to manage operational management processes.

Many organizations using non-Microsoft platforms use third-party systems management software to monitor their computing resources. Product connectors are the primary means of enabling coexistence between MOM and other monitoring solutions. Product connectors are implemented using the MOM Connector Framework (MCF). The MCF is also used as the technology basis for connecting MOM management groups together.

More than 100 management packs and product connectors are provided by various companies that interact with MOM, in addition to those offered by Microsoft. With so many existing third-party management packs and connectors (and with all the new ones being written), it isn't practical to write about each of them here—we instead will highlight several key areas. We will discuss hardware management packs provided by several hardware vendors. We will also examine approaches to using management packs to monitor non-Windows systems and devices, and highlight some third-party application management packs.

Finally, we will discuss five of the six solution accelerators available for MOM 2005. The sixth solution accelerator is the MOM 2005 SLA Scorecard for Exchange, which we talked about in Chapter 17, "Managing Microsoft Messaging." These accelerators provide predefined solutions to extend MOM's capabilities utilizing ITIL-based best practices.

Talking to the Rest of the World

MOM 2005 is not limited to managing and monitoring Microsoft software environments. MOM instead incorporates far greater applicability and extensibility, which is logical because most companies do not exclusively run Microsoft products. Network components exist that provide routing and switching functions, and many organizations use other operating systems such as UNIX (including HP-UX, AIX, Linux, Solaris, and SCO) and hardware platforms such as Sun and IBM's AS/400 and RS/6000. By utilizing product connectors and additional management packs, MOM 2005 can provide a single monitoring solution that will monitor hardware, non-Windows servers, network devices, and third-party applications, in addition to monitoring Microsoft applications and operating systems.

MOM can also interact with other management systems. In a simple MOM 2005 implementation you have a single server running MOM, hosting both the management server and the OnePoint database (and potentially the reporting services and reporting databases). This configuration may be appropriate if you are only monitoring a small number of systems. Large organizations with thousands of MOM agents often will install the MOM database on a separate server and also use an Enterprise Console from a third-party management suite such as the Tivoli Enterprise Console (TEC), one of the Hewlett-Packard (HP) products, or Computer Associates (CA) Unicenter. Customers using a third-party management tool will need to integrate MOM with their existing environment. As a player in the Enterprise Systems Management space, MOM must have a mechanism to connect to and communicate with other management systems, including additional MOM management groups, third-party management systems, and problem management systems. The MOM Connector Framework enables this level of integration.

Comparing MOM to Other Enterprise Monitoring Solutions

Although it is beyond the scope of this book to compare each enterprise console to MOM 2005's functionality, it is relevant to position the advantages of Operations Manager versus other Enterprise solutions. Why should we use MOM instead of another management tool? The primary areas where MOM excels are

- Product knowledge created by the Microsoft product groups and Microsoft Consulting Services (MCS) is included in each of the Microsoft management packs.
- The Microsoft Connector Framework allows MOM to connect to other systems for integration with other Enterprise monitoring solutions.
- MOM integrates with no-cost hardware management packs from Dell, Hewlett-Packard, and other hardware vendors.

- MOM supports customizing management packs to further extend its capabilities. We discuss this further in Chapter 20, "Developing Management Packs."
- Third-party organizations provide management packs, which increase MOM's monitoring capabilities.

The MOM Connector Framework

The MOM Connector Framework is the core infrastructure platform for implementing interconnections with other software products. In its simplest form, the MCF is a web service your connector can use as a communications interface. The MCF enables full bidirectional alert forwarding and synchronization between MOM and other management systems. The MCF is a managed .NET class library that provides the underlying infrastructure required to build connectors. The MCF includes the MCF application programming interface (API), used to receive new or updated data and store that data.

Installing the MOM Connector Framework

You can install the MCF during the initial setup of your MOM management group or add it later through modifying your MOM configuration using Add/Remove Programs from the Control Panel or by running setup.exe from the MOM installation media.

MCF Installation Prerequisites

Internet Information Server (IIS) and ASP.NET are prerequisites for installing the MCF and should be installed on your management server prior to adding the MCF.

The following are the required steps to install the MCF in an existing MOM configuration:

1. Navigate to Control Panel on the Management Server. Open Add or Remove Programs, select Microsoft Operations Manager 2005, and click on the Change button. From the Microsoft Operations Manager 2005 Setup Welcome screen, select Next. As shown in Figure 19.1, you are given the options to Modify, Repair, or Remove MOM 2005. Select Modify.
2. The MOM 2005 Custom Setup screen shows the options to add or remove components. Because we are adding the MCF, left-click on the red X next to the MOM Connector Framework component. Figure 19.2 displays the MCF component selected for installation.
3. The MOM setup process next initiates the prerequisite checker. If Internet Information Server (IIS) is already installed, your environment should meet the hardware and software prerequisites because it is an existing MOM installation; if not, correct the errors and rerun the MOM setup program. After passing the installation prerequisites, you are ready to install the MCF.

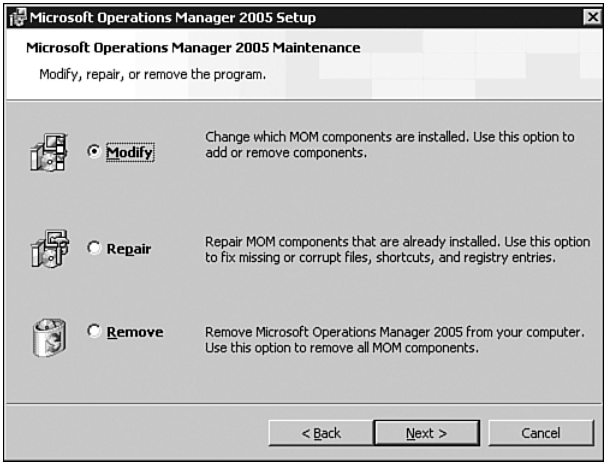


FIGURE 19.1 The Modify option of the MOM 2005 Setup screen.

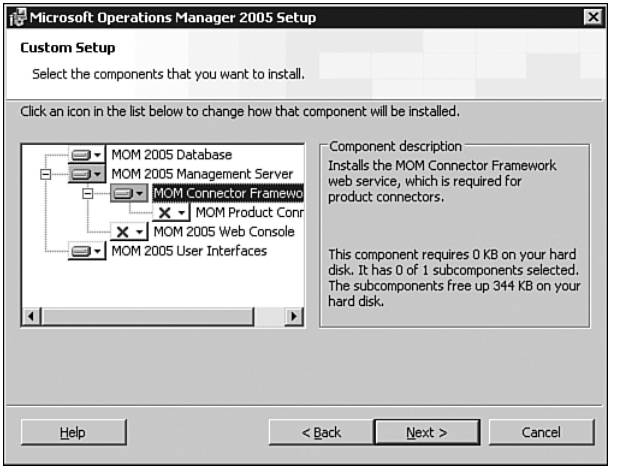


FIGURE 19.2 Selecting the MOM Connector Framework Component for install.

4. Make sure that the MOM 2005 installation media is available; you will need the momserver.msi file to complete the installation. Upon completion, the Setup program displays the Complete screen. Click Finish to end the setup process.

Verifying the MOM Connector Framework

Now that the MCF is installed, we recommend you verify that it is responding properly. The MCF installs a web service that by default listens on port 1271. An easy way to verify the functionality of the MCF is by specifying its URL using a web browser such as Internet Explorer. The default URL for the MCF is http://<*server name*>:1271/connectorservicev2.asmx.

Figure 19.3 shows the default MCF web page displayed using the preceding URL. If the MCF is functioning, this screen will display properly.

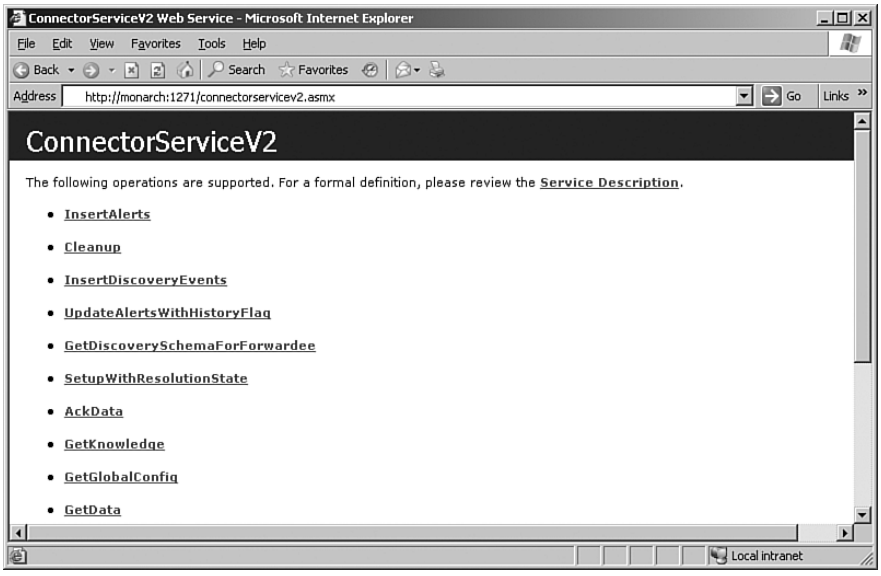


FIGURE 19.3 The default MCF Web page.

Web Services Used by the MCF

The MOM 2005 version of the MCF actually includes two separate web services: the 2005 version used by the MOM-to-MOM Product Connector (MMPC) accessible at http://<*server name*>:1271/connectorserviceV2.asmx, and the MOM 2000 version at http://<*server name*>:1271/connectorservice.asmx.

Changing the Port Number

You can change the default port number after installation using the following procedure (for this example we will change the port on our Monarch management server):

1. Open the IIS Manager, located under Administrative Tools. Within the IIS Manager MMC console, navigate to the Web Sites folder; left-click on it to select that folder.
2. The folder displays the websites available on the server. To change the port of the MCF web service, right-click on the Microsoft Operations Manager 2005 Connector Framework website and select Properties.
3. The Transmission Control Protocol (TCP) port is listed on the Web Site tab. Change the TCP port to the desired port number and click OK to apply the change. Figure 19.4 shows the MCF web application listening on port 1281.

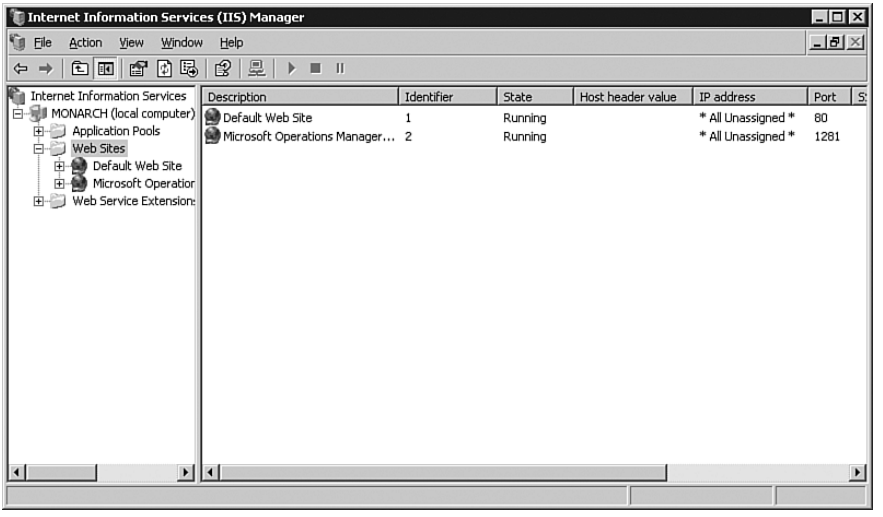


FIGURE 19.4 The IIS Manager showing the MCF Web Application on Port 1281.

Remember to Change the Port!

Make sure that the URL is changed to the appropriate port when testing the MCF web application. In this case the new URL for our Monarch server is http://monarch:1281/connectorservice2.asmx.

The MOM-to-MOM Product Connector

With the MOM Connector Framework functional, you can now install connectors. A *connector* is an application that uses the MCF to send and receive data between the management group and another management application, such as another MOM management group or third-party software. You can send and receive alerts and discovery data between MOM and other applications such as other MOM management groups, problem management systems such as BMC's Remedy or Peregrine's Service Center, or third-party Enterprise consoles. One of the main connectors to use the MCF is the MOM-to-MOM Product Connector (MMPC).

MMPC Scheduled for Changes?

Information from Microsoft indicates that the MMPC will be obsoleted in future versions. However, the MCF capability will continue to be used to communicate with monitoring systems external to Operations Manager, and equivalent functionality to the MMPC will be available in the next version.

The MMPC sends alerts and discovery data between two MOM management groups. You can configure alert data to be sent bidirectionally between the source management group

and the destination management group, or to forward the alert information only one way to the destination management group. Chapter 10, "Complex and High Performance Configurations," discussed scenarios where multiple management groups would be necessary, whereas Chapter 5, "Planning Complex Configurations," talked about when the MMPC may be required for your environment.

Bidirectional MMPC Communication Defined

Bidirectional communication for the MMPC means that alerts that originate in the source management group are sent to the destination management group, and updates are synchronized in both directions. An alert originating in a destination management group will not appear in the source management group unless you configure an MMPC connection that points in the other direction, but this is rarely done.

Source and destination management groups can form a hierarchy where alerts from one management group are forwarded to another. Forwarding alerts enables MOM to support multitiered configurations allowing organizations with multiple locations to centralize alerting with a destination management group.

The decision to send data bidirectionally or only one-way depends on your particular implementation of MOM. You may want to enable bidirectional forwarding of alert data to send all alerts to a destination management group, which will be used as the single console for your operations staff. The bidirectional capability sends the updates applied at the destination management group back to the originating management group, including alert history and alert properties entered at the destination management group.

You may consider using a connection that forwards alerts in only one direction when information from the source management group is relevant to the administrators of the destination management group but the destination management group does not take actions to resolve those alerts. Let's take an example where the source management group monitors only network equipment, and the destination management group monitors the servers and applications. Network problems impact the operating system and applications, so administrators in the operating systems/applications management group will want to be aware of issues, but the administrators of the network management group are responsible for resolving those alerts.

Management Pack Requirements with the MMPC

Using the MMPC requires that all management packs installed in the source management group also be installed in the destination group, and that any custom rules in the source group must exist identically in the destination group.

Discovery Information

Discovery information can be forwarded from the source management group to the destination management group only (not bidirectionally). You have options as to what data to send to the destination management group including the Computer class properties, all

discovery data, or a customized set of discovery data you specify. We will discuss this in more detail as we configure the connector in the next section of this chapter.

The MOM 2005 Deployment Guide

Implementing multitiered management groups is documented in Chapter 9, "Creating Multitiered Management Groups," of the Microsoft Operations Manager 2005 Deployment Guide. The Deployment Guide can be downloaded from the Microsoft Download Center at http://www.microsoft.com/downloads. Search for "MOM 2005 Deployment Planning Guide."

Installing the MOM-to-MOM Product Connector

Setting up the MOM-to-MOM Product Connector uses the same process we used to install the MOM Connector Framework. The MMPC can be installed when you initially install the management group, or it can be added after the management group is installed and running. To install the MMPC after creating the management group, perform the following steps:

1. Navigate to Control Panel and open Add or Remove Programs. Select Microsoft Operations Manager 2005 and click on Change. Select Next at the Welcome screen, and Modify at the next screen.
2. At the Custom Setup screen select the MOM Product Connector by left-clicking on the MOM Product Connector drop-down menu and choosing the option to install this component. Figure 19.5 shows the Custom Setup screen with the MOM Product Connector selected. (The MCF and the MMPC can be installed at the same time.)

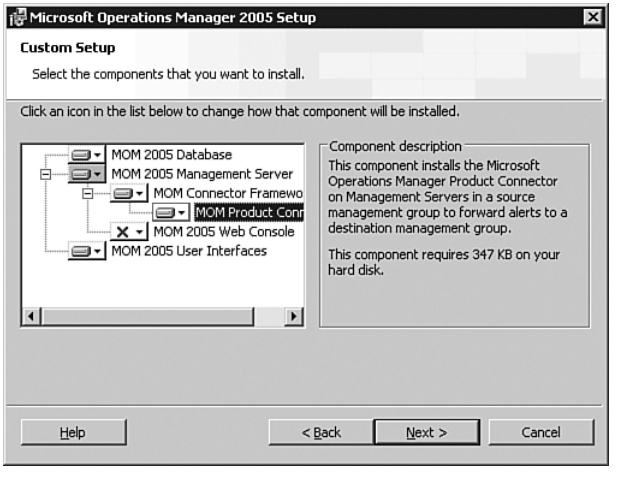


FIGURE 19.5 Custom Setup with the MOM Product Connector selected.

3. Selecting Next invokes the prerequisite checker, which should run successfully if the management group and MCF are installed. It there are errors, correct them and rerun the setup program.
4. At the next screen you are asked to enter the DAS account. Use the same account previously specified for your management group as the DAS account.

   This account must be a member of the MOM Administrators local group on the local management server and all other management servers that the product connector will talk to, including the management servers in both the source and destination management groups.
5. Select Next. The account credentials are verified, and the Ready to Modify screen is displayed. Select Install to continue. At the Setup Complete screen, select Finish to exit the MMPC setup wizard.

Using Three-Tiered Management Groups

As previously discussed in Chapter 5, MOM 2005 can support a three-tiered management group hierarchy. With a three-tiered approach, the middle tier receives alert data from the bottom tier management group and will forward alert data to the top tier management group.

Configuring the MOM-to-MOM Product Connector

With the MMPC component installed, you can now configure it to forward alert data and discovery data to a destination management group. Let's step through the procedure to configure the MOM-to-MOM Product Connector.

Individual connectors are defined with the MOM 2005 Administrator console under Administration \ Product Connectors. Right-click and select Create MOM-to-MOM Connection, shown in Figure 19.6, to launch the Create MOM-to-MOM Connector Wizard.

1. The first screen after the Welcome screen is the Connector properties screen displayed in Figure 19.7.
   - The first entry in the MMPC properties screen is the name of the connector. The name should be descriptive of what we will connect to. Our example will connect to the Group2 management group on the Durango server, so we name the connector Connect to Group2.
   - The next entry is the resolution state ID. Alerts are forwarded to the destination management group based on the Alert resolution state. Use the default Alert resolution state of 150; we will look at resolution states in more detail in the next section.
   - The final entry on this screen is the polling interval in seconds of how often MMPC checks for new alerts or alert changes. The default is every 20 seconds.

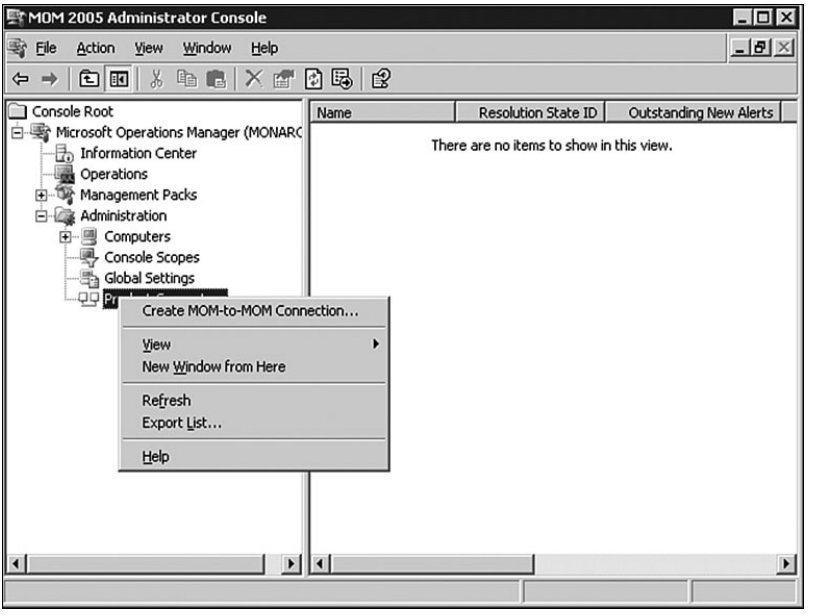


FIGURE 19.6 Create a MOM-to-MOM Connection in the Administrator console.

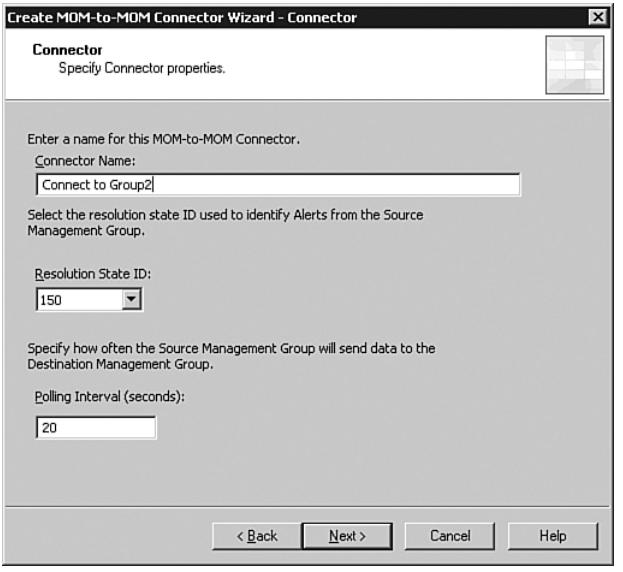


FIGURE 19.7 The MMPC properties screen.

Defining Resolution States

You cannot use a resolution state that is already defined. Defined resolution states are not listed in the drop-down of available resolution states when creating a connector.

Existing resolution states can be found in the MOM 2005 Administrator console, under Administration \ Global Settings \ Alert Resolution States.

3. Next you proceed to the Add MOM Master Management Group screen.
   - Enter the name of the management server in the destination management group hosting the MCF web service.
   - If the MCF on the destination management server listens on a port other than the default of 1271 you must specify the target MOM web service rather than the name of the management server.
   - The final check box is necessary when the target management server is running MOM 2000 SP1.

   Our example in Figure 19.8 specifies Durango as the Target MOM Management Server.

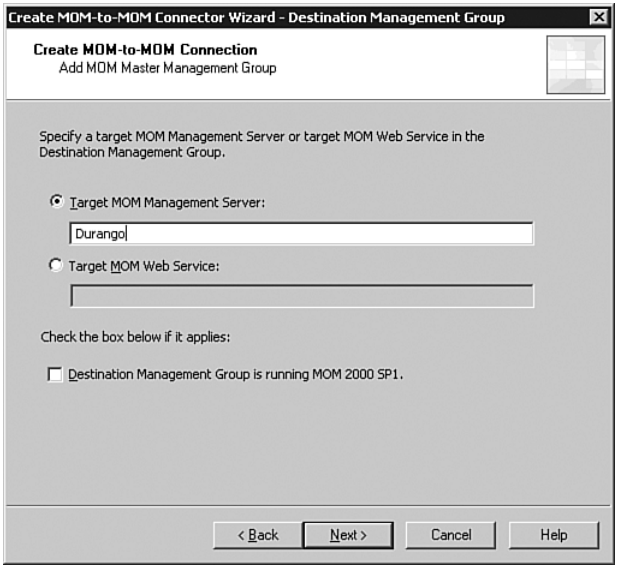


FIGURE 19.8 Add the MOM Master Management Group.

Installation Requirements for the Destination Management Server

The destination management server must at a minimum have the MCF installed. If the destination management group will also function as a source management group (forwarding alerts and discovery data to another destination management group), it requires both the MCF and the MMPC. If the destination management group does not forward alerts and discovery data to another destination management group, only the MCF is required.

4. At the Forwarding Properties page, specify what to forward and indicate whether you want bidirectional alert forwarding. The first check box determines whether you will forward alerts and alert updates to the destination management group.

   As a subset of this functionality, you can specify whether you want alert updates to flow back down to the source management group. As we discussed earlier in "The MOM-to-MOM Product Connector" section, you may want alert updates to flow back to the source management group if that information would be utilized by the operations staff using the MOM Operator console for that management group. If your operations staff only uses the Operator console at the destination or top-level management group, you may decide not to have alert updates flow back down to the source management group.

   The Forwarding Properties screen also gives you the option to forward discovery data. This capability enables the top-level management group to display an accurate view of the state of the enterprise. Forwarding discovery data enables the State views to correctly display the agents and their alerts forwarded from the source management group. Within the option to forward discovery data, you also can specify the type of discovery data you want to forward:

   - The Forward Only the Computer Class and Associated Properties radio button forwards service discovery information associated with the computer class.
   - By contrast, the Forward All Discovery Information option allows all service discovery information to be forwarded introduced by any additional installed management packs.
   - Forward Only a Custom Set of Discovery Information allows for an input file that contains only those attributes you want to forward. In the example shown in Figure 19.9, we selected to forward all discovery information to the destination management group.

5. Next is the MMPC failover configuration screen. You can configure the destination management group with multiple web services for increased reliability. For instance, if you have more than one management server, you can install the MCF on each management server in the destination management group. The failover configuration screen allows you to specify the order of priority for the additional servers if a management server fails. In this example, the Group2 management group only has one management server (one web service), so it is the only server listed. Figure 19.10 shows the failover configuration screen.

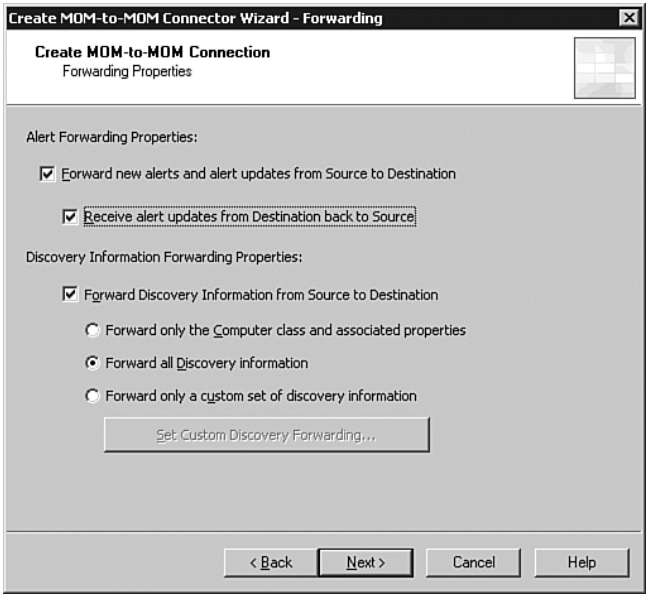


FIGURE 19.9 MMPC forwarding properties.

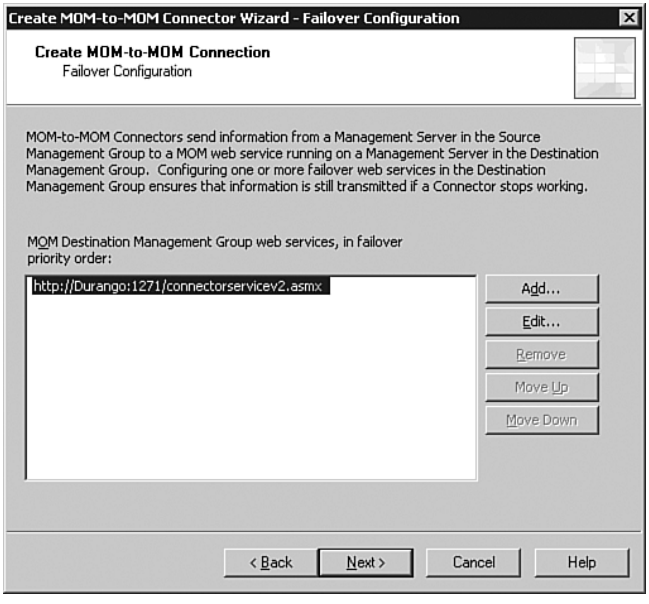


FIGURE 19.10 The Failover Configuration screen.

6. On the Confirmation screen (see Figure 19.11), you can review the settings or go back and make changes as necessary.

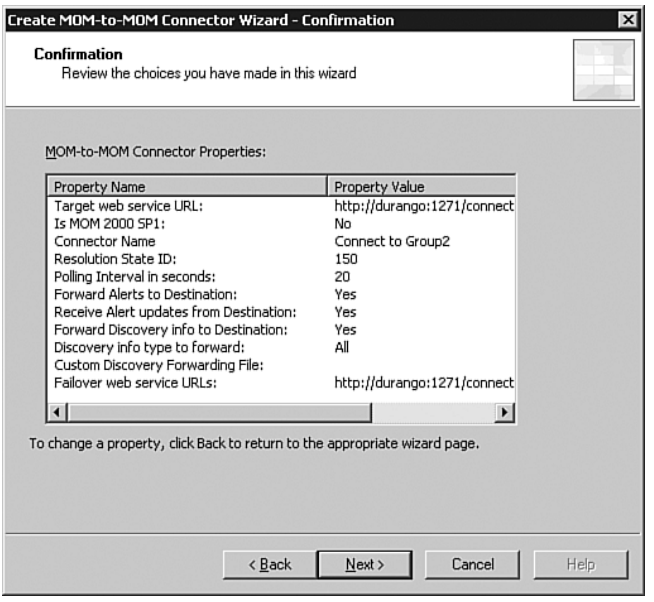


FIGURE 19.11 The Confirmation screen.

7. From the Confirmation screen you proceed to the Completion screen. The MMPC is now successfully created. Click Finish to end the MMPC wizard; the MMPC is now ready to use.

Using the MOM-to-MOM Product Connector

After installing the MMPC, you configure MOM to use the MMPC. The MMPC runs as a service called MOM-to-MOM Connector that polls the local MCF, which then polls the OnePoint database. The MCF is polled every 20 seconds by default to check for new alerts with the alert resolution state specified during installation (the polling interval is configured when you create the connector). If you do not remember the alert resolution state, check the MOM 2005 Administrator console under Administration \ Product Connectors. In Figure 19.12, our Connect to Group2 connector has a Resolution State ID of 150.

For the connector to forward an alert to the destination management group, the alert must have the specified alert resolution state. (Attribute discovery does not necessarily follow these rules; we will discuss how it works later in this section.)

The initial resolution state of an alert is New. There are several ways to change the resolution state, which enables forwarding the alert. You can manually change the alert in the MOM 2005 Operator console or use the "a script runs as a response" option in an alert processing rule. The MOM 2005 Management Pack contains an alert processing rule specifically for this purpose, located under Management Packs \ Rule Groups \ Microsoft Operations Manager \ Operations Manager 2005 \ Connector Framework \ Mark Alerts for forwarding to MOM master management group.

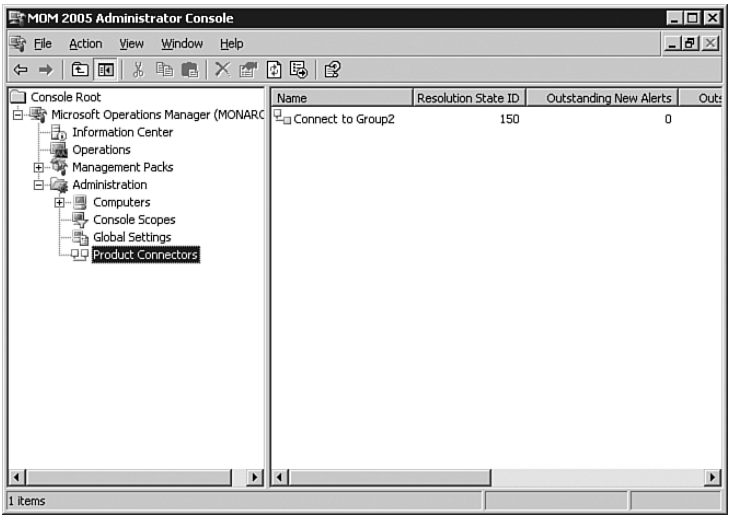


FIGURE 19.12 Product Connector properties in the Administrator console.

The Mark Alerts for forwarding to the MOM Master management group rule is initially disabled by default. When enabled, the rule changes all alerts of error severity or higher to the alert resolution state necessary for the MMPC.

Enabling the Mark Alerts for Forwarding Alert

This rule will generate errors if enabled before the MMFC is configured because resolution state 150 is not yet defined. You should verify that the rule group this rule belongs to is associated with the computer groups you want to forward alerts from.

The response this rule uses is a script also named MOM Mark alerts for forwarding to MOM Master management group. The script changes the resolution state to the state necessary (150) for the MMPC:

```
MOM Mark alerts for forwarding to MOM Master management group
Option Explicit
Sub Main()
   Dim myAlert
   'change resolution state
   Set myAlert = ScriptContext.Alert
   myAlert.ResolutionState = 150
End Sub
```

At the next polling cycle for the MOM-to-MOM Connector service, any alert with a resolution state of 150 is forwarded to the destination management group. The alert arrives with an alert resolution state of New, allowing alert processing rules at the destination management group to act on the new alert. The history stored with the alert reflects that

it was forwarded from the source management group. If bidirectional forwarding is configured, any changes to the alert are sent back down to the source management group.

As mentioned earlier in this section when we installed the connector, state-based management incorporates attribute discovery and forwarding. A caveat is that any state-based alert is forwarded to the destination management group, regardless of the alert processing rules in place to change the alert resolution state of an alert.

Let's take an example where the MOM Mark Alerts for forwarding to MOM Master management group rule is used to mark that only alerts of Error or higher are forwarded to the destination management group. If a state-based alert is generated with a severity of Informational, the alert is forwarded regardless of its severity. This behavior is necessary for the state to be reflected accurately at the destination management group. For instance, if a state-based alert is generated with a Success severity; the alert must be forwarded to the destination group for the state to change to Success for the server role defined in the state based alerts.

More information on state-based alerts is discussed in Chapter 14, "Monitoring with MOM."

The MOM-to-MOM Product Connector in an Untrusted Environment

Configuring the MOM-to-MOM Product Connector is somewhat straightforward in a trusted environment. The MOM-to-MOM Connector service uses the DAS account credentials to write the data to the destination management group.

The process differs when the destination management group is in an untrusted domain (or an untrusted forest). In this case, a server certificate from the destination management server is used to authenticate the MCF-based product connector. More generally, the setup process involves obtaining a user certificate for the source management server and placing it into a folder designated by the MOM-to-MOM Connector service. On the destination management server you must obtain and install a server-based certificate, configure the MCF website to use Secure Sockets Layer (SSL) and require a certificate, and then map the user certificate from the source management server to the DAS account. The steps required to enable the MMPC to send alerts to an untrusted source server are discussed in the following sections.

Obtaining a Server Certificate We start by obtaining a certificate from the certificate server:

1. Obtain a server authentication certificate from a certificate server (http://*<certificate server machinename>*/certsrv). The name of the certificate must be the Fully Qualified Domain Name (FQDN) of the destination management server. Store the certificate in the local computer certificate store.
2. On the certificate server used in step 1, open the Certificate Authority MMC, expand Issued Certificates, and open the certificate that was generated in the previous step. Select the Details tab, click Copy to File, and save the certificate to a file. Note the path you save the file to and the name of the certificate.

3. Copy the .cer file just created in step 2 to the destination management server.
4. Using the Certificates MMC snap-in on the destination management server, import the certificate (the .cer file from step 3) into the Personal certificates folder.

   You can access the Certificates MMC by selecting Start, Run, type **mmc.exe**; selecting File, Add/Remove Snap-in; and selecting Certificates.
5. From the destination management server, connect to the certificate server specified in the first step (http://*<certificate server machinename>*/certserv) and click on Download a CA Certificate, Certificate Chain, or CRL; then select Install this CA certificate chain.

Configuring the MCF Website on the Destination Server Now we can configure the MCF website on the destination management server to use SSL and the newly created certificate:

1. Using the IIS Manager on the destination management server, go to the properties page of the Microsoft Operations Manager 2005 Connector Framework website. Select the Directory Security tab, click the Server Certificate button, and select Assign an Existing Certificate.
2. Choose the certificate you installed in the previous section and specify port 443.

Creating a Client Authentication Certificate at the Source Server At the source management server we will create and install a client authentication certificate:

1. On the source management server, log on as the administrative account that will install the connector.
2. On the source server request a certificate from the certificate server (http://*<certificate server machinename>*/certsrv), using an advanced certificate request.

   The type of certificate is Client Authentication. Name the certificate MOM MMPC. Do not choose to store the certificate in the local computer store. Do not select Export the Private Keys, and do not save the keys to a file. Select Submit. After the certificate is issued, navigate back to the certificate server and install the certificate accepting all defaults.
3. Navigate to the certificate server again, and select Download a CA certificate, certificate chain, or CRL. Select Install this CA certificate chain to install the certificate.

Exporting the Certificate Now that we have the certificate, we need to export it to both a .pfx and .cer file, copying the .cer file to a folder for MOM:

1. Using Internet Explorer on the source management server, select Tools, Internet Options, Content, and click Certificates. You should see the client certificate MMPC. Click Export and select Yes; export the private key and accept the defaults; enter a password of your choosing and save the file as c:\mmpc.pfx.

2. Run Export again. This time do not export the private key. Select the DER encoded binary x.509 (.CER) format. Save the file as c:\mmpc.cer.
3. On the source management server, create a folder called ConnectorService under the folder pointed to by HKEY_LOCAL_MACHINE\SOFTWARE\Mission Critical Software\OnePoint\DATADIR. This is typically *%Installation Root%*\Documents and Settings\All Users\Application Data\Microsoft\Microsoft Operations Manager\.

Copying and Mapping the Certificate at the Destination Server We will now copy the .cer file to the destination management server, mapping the certificate to the DAS account:

1. Copy the c:\mmpc.cer file to the ConnectorService folder, renaming it to ClientCertificate.cer. Copy ClientCertificate.cer to the destination management server as well.
2. Log on to the source management server using the DAS account. Open Internet Explorer and select Tools, Internet Options, Content, and select Certificate. Select Import and choose the c:\mmpc.pfx file, accepting the defaults. Place the certificate into the personal store.

Configuring the MCF Website for SSL Finally, we configure the MCF website to use SSL and the client certificate, mapping the certificate to the DAS account:

1. Log off as the DAS account and log on as the administrative account that will install the connector.
2. Using the IIS Manager on the destination management server, configure the properties of the Microsoft Operations Manager 2005 Connector Framework Web Site. Under the Directory Security tab, select Edit. Click the Require Secure Channel (SSL) check box and select the Require Client Certificates radio button. Click on the Enable Client Certificate Mapping check box as well.
3. Click Edit to configure the client certificate mapping. Map the certificate (ClientCertificate.cer) to the MOM DAS account used on the destination node.
4. Restart the MCF website on the destination management server. The certificates are now configured and ready for use.
5. Configure the connector to use the secure MCF website. On the source management server, open the MOM 2005 Administrator console and navigate to Administration \ Product Connectors. Configure the MMPC specifying the Target MOM Web Service as https://*<destination server FQDN>*/connectorservicev2.asmx.

More Information on Certificates

More information about generating and installing certificates is available in the IIS help files.

Connecting to Third-Party Management Suites

A number of connectors and other resources are available for using and extending the MCF. Product connectors extend the monitoring benefits of MOM 2005 by allowing the transfer of information between third-party management software packages and MOM 2005. Microsoft provides a number of product connectors that enable communication between some of these products and MOM. The following are examples of connectors that currently exist:

- Tivoli—Allows alerts to be forwarded to Tivoli TEC and synchronized between MOM and Tivoli.
- HP OpenView—Provides unidirectional and bidirectional communication between MOM and HP OpenView.
- HP Network Node Manager—Configures MOM to send alerts to HP Network Node Manager.

These connectors are architecturally similar to the MOM-to-MOM Product Connector in that they run on the MOM Connector Framework and forward alert and discovery data to the third-party management application, with the objective of providing a single enterprise view of your infrastructure.

Other resources available for using and extending the MCF include:

- MOM Connector Framework Class Library—The MOM 2005 SDK contains the programming examples and API details necessary to utilize the MOM Connector Framework Class Library, allowing you to build your own connector and access alert data from MOM. The MOM 2005 SDK is available at http://go.microsoft.com/fwlink/?linkid=50272.
- The Autoticketing Solution Accelerator describes the process of building a connector between MOM 2005 and a generic problem ticketing system. The Solution Accelerator describes the phases and layers of building a business model for trouble ticket generation and incident management. The Autoticketing Solution Accelerator is available at http://go.microsoft.com/fwlink/?linkid=50277. We discuss this solution accelerator further in the "Autoticketing Solution" section later in this chapter.

Hardware Management Packs

Hardware management packs allow you to manage and monitor the hardware in your server environment using the MOM interface as a single systems management tool, and include product knowledge from the hardware vendor integrated into MOM.

For monitoring server hardware, a number of hardware vendors provide management packs that integrate their monitoring environment and capabilities into MOM. The integration allows you to view the information collected using the MOM 2005 Operator console and integrate alert management with that provided by MOM.

Dell, HP, IBM, Fujitsu, and Unisys currently offer hardware management packs. Check the Management Pack Catalog at http://go.microsoft.com/fwlink/?linkid=43970 (see the "IBM" section later in this chapter for an exception to this) for a list of management packs currently available.

Each of these management packs provide integrated status information on the health of the hardware. These management packs are available at no cost for download using the links at the Management Pack Catalog. Typically you will need to install both the MOM agent and the corresponding vendors' agent (for Dell OpenManage, HP Insight Manager, IBM Director, Fujitsu ServerView, or Unisys Server Sentinel) on each monitored server.

Dell

The Dell management pack gathers information generated by the Dell agents and integrates that with MOM. Using the Dell management pack with MOM provides a single interface to monitor both hardware and software, offering a comprehensive solution. Dell's integration with MOM is illustrated in Figure 19.13, which shows the state of various components and subcomponents monitored by the Dell agent.

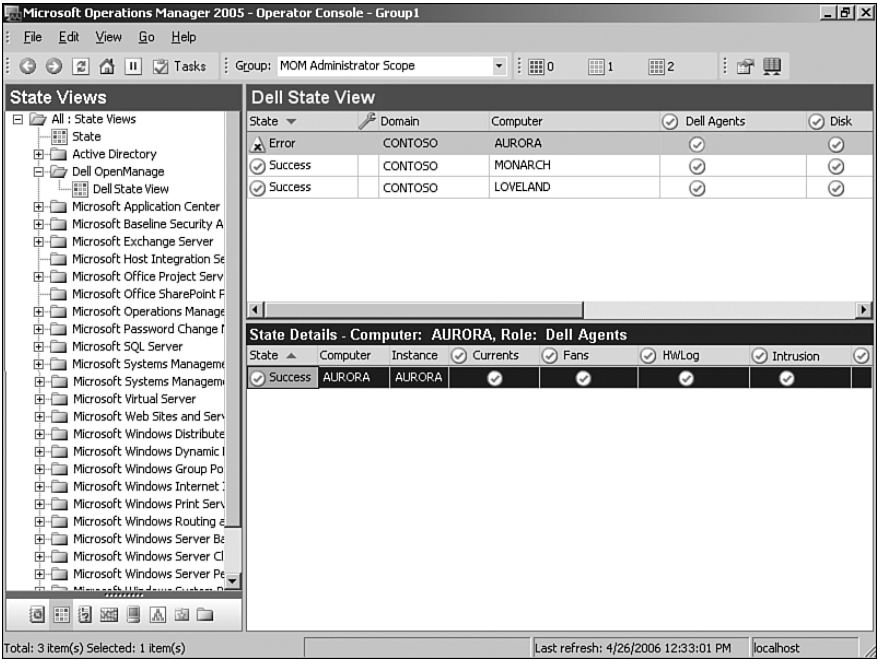


FIGURE 19.13 The Dell State view in the Operator console.

Similar to other management packs we have discussed in this book, Dell also includes product knowledge that provides recommended approaches for resolving issues identified by the management pack.

The state of Dell components is periodically refreshed every 10 minutes or on receipt of alerts from the Dell instrumentation. To manually launch this update process the Dell management pack includes a task called the Update Dell State View. This task launches the Task Wizard, which updates the State view to one of the standard MOM conditions: Normal/Green, Warning/Yellow, Critical/Red, Not Applicable/White, and Unavailable/Gray. MOM shows the status of the task with an event that can be viewed within the Operator console.

HP

HP provides multiple management packs that include

- HP Integrity (manages the HP Integrity server line)
- HP ProLiant (manages the HP ProLiant server line)
- HP Insight (obsoleted by the HP Integrity and HP ProLiant management packs)
- HP Storageworks (manages the HP Storageworks products)

The HP Integrity and ProLiant management packs perform the same actions as the Dell management pack, but for HP/Compaq hardware—including providing HP-specific product knowledge. Figure 19.14 shows an example of the HP integration with MOM.

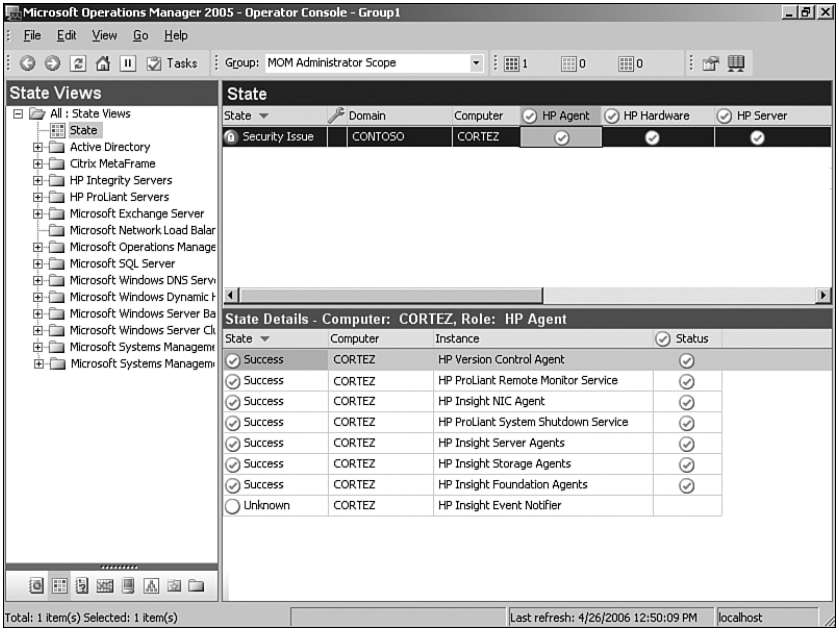


FIGURE 19.14 The HP State view in the Operator console.

The HP management packs include a number of tasks that can be initiated from the MOM Operator console. The tasks enable you to gather information and access browser links to the remote systems:

- HP System Management home page—Opens a web browser link that provides information for your specific type of HP server including system hardware health, configuration, performance, and status information.
- HP Systems Insight Manager—Opens a web browser link that launches the HP Systems Insight Manager on the HP server specified.

- HP Lights-Out Management Processor (ProLiant)—Collects HP Lights-Out Management Processor data and provides a browser link to remotely access the server.
- HP Management Processor (Integrity)—Collects HP Management Processor data and provides a browser link to remotely access the server.
- Computer Model Discovery—Enables you to manually discover and classify HP ProLiant servers. The process identifies the model of the server and reclassifies it into the correct HP computer group. By default this event executes every 30 minutes; using this task enables you to manually initiate the process.

Dell and HP on Non-Windows Operating Systems

If you have non-Windows Operating Systems running Dell or HP hardware, you can use MOM to monitor those systems with eXc Software's Virtual Agents for Dell and HP. More information is available in the Management Pack Catalog.

IBM

IBM provides a management pack that integrates with the IBM Director 5.1 agent. At the time this chapter was written, a link to this management pack was not listed at the Management Pack Catalog website. IBM provides details of the installation process at http://publib.boulder.ibm.com/infocenter/eserver/v1r2/index.jsp?topic=/diricinfo/fqm0_t_installing_ibm_director_uim_for_mom.html.

The IBM management pack is referred to as the "Upward Integration Module for MOM" and adds capacities similar to those provided by Dell and HP, including a State view that provides the status of the hardware components in the system.

Additional information for this management pack is available at http://www-03.ibm.com/servers/eserver/xseries/systems_management/ibm_director/upward/features/mom.html.

These links are also available in Appendix E, "Reference URLs."

IBM Hardware Monitoring with eXc

eXc has developed management packs to assist in monitoring IBM hardware. The management packs include the following:

- Virtual Agent for IBM BladeCenter—Provides monitoring of all SNMP-capable BladeCenter products
- Virtual Agent for IBM FastT Storage—Monitors IBM FastT storage, which provides midrange storage solutions
- Virtual Agent for ESS Storage—Monitors IBM Enterprise Storage System equipment (also known as the Shark), which provides high-end storage solutions

Free 30-day evaluation versions of eXc's management packs and additional information about eXc are available at www.excsoftware.com.

Fujitsu/Siemens

Fujitsu offers a management pack for monitoring Fujitsu/Siemens PRIMERGY hardware in a Microsoft environment. Fujitsu's system management tool is called ServerView. Similar to the management packs from Dell and HP, the ServerView agent is required on systems you will monitor using MOM. Additional information on the Fujitsu management pack is available at: http://manuals.fujitsu-siemens.com/serverbooks/content/manuals/english/sv_integration-e.pdf. Although reports and tasks are not currently available as part of the Fujitsu management pack, the documentation includes the steps to create ServerView tasks you can run from the MOM Operator console.

Unisys

Unisys' line of ES7000 series servers is often used with Windows Server 2003 Datacenter Edition implementations. Unisys' management pack for their ES7000 series incorporates alert monitoring from the Unisys Server Sentinel with MOM 2005. The Unisys management pack is a no-cost item for customers with a Unisys support agreement and integrates hardware and environmental error information into MOM. The first version of the Sentinel management pack for MOM 2005 monitors systems running Server Sentinel 2.2 or later. The management pack includes

- Automatic monitoring of all Server Sentinel systems monitored by a Sentinel Management Server
- Tasks collecting and removing Server Sentinel diagnostic data
- Automatically notifying the Hardware Support MOM notification group of critical errors
- Public views that observe all Server Sentinel alerts and events, Server Sentinel systems, and status of Server Sentinel systems
- Automatically detecting 32-bit ES7000 servers on which the MOM agent is installed
- Ability to directly launch the Server Sentinel Web pages from any Server Sentinel alert

Additional information on this management pack is available at the Management Pack Catalog (select Unisys in the dropdown box for the company offering the product) or you can access Unisys' information directly at http://www.unisys.com/products/enterprise__servers/high_d_end__servers/system__software/unisys__server__sentinel/mom.htm.

Non-Windows Server Management Packs

Several options are available for using MOM to monitor non-Windows server systems. One option is to use the MOM SNMP and WMI SNMP providers to collect traps and SNMP data from the non-Windows system. Alternatively you could utilize the MOM syslog provider to collect information and create rules for specific syslog events. Another option is to implement third-party software to monitor your other operating systems.

Third-party options, such as those discussed in the "Hardware Management Packs" section earlier in this chapter, provide solutions that identify information relevant to MOM. Currently four vendors provide monitoring resources for non-Windows systems: Engyro, eXc, Jalasoft, and Quest.

Table 19.1 provides a summary of the operating system monitored by each vendor (ordered alphabetically), which we will then describe in greater detail.

TABLE 19.1 Vendor and Operating Systems Monitored

Vendor	Operating Systems Monitored
Engyro	Linux, UNIX
eXc	AS/400, Linux, Unix, MAC, SCO
Jalasoft	Linux
Quest	Linux, MAC, Unix

Engyro

Engyro provides connectors that can provide monitoring for Linux and other UNIX systems including HP-UX, IBM-AIX, and Sun Solaris. Information on Engyro and evaluation versions is available on the website located at www.momconnectors.com.

eXc

eXc provides monitoring for AS400, Linux, UNIX, MAC OS X, and SCO operating systems, which integrate with MOM. eXc relies on a virtual agent that uses a custom WMI event provider to communicate with MOM 2005.

The eXc MOM 2005 management pack incorporates AS400, Linux, UNIX, MAC, and SCO information into your MOM 2005 environment. A free 30-day evaluation version of the eXc solution and additional details about eXc are available at www.excsoftware.com.

Jalasoft

Most of the Jalasoft management packs monitor network-related devices, so we delay their discussion until the "Network Management Packs" section later in this chapter. Nevertheless, Jalasoft also has an agent that functions on Linux and can integrate with MOM 2005. The Jalasoft architecture uses several key server roles for its solution including

- Network Manager Server (NMS)—Monitors and collects information
- Network Scan Server (NSS)—Scans the network to add supported devices
- Data Server (DS)—Gathers device data from the NMS and forwards to the Xian Connector
- Xian Database—A SQL backend database that stores information for the Jalasoft product
- Xian Connector for MOM 2005—Relays information to MOM via the Microsoft Connector Framework (MCF)

A free 60-day evaluation version of the Jalasoft Linux Agent for 2005 (which allows a user to run one Network Manager Server and discover up to 10 devices) and additional information on Jalasoft is available from its website at www.jalasoft.com.

Quest

Quest's Management Xtensions for MOM (QMX) provides a method to integrate Linux, UNIX, and MAC OS X systems into MOM 2005. The Quest Management Packs monitor the UNIX, Linux, and Mac operating systems (CPU, memory consumption, swap utilization, storage, network), generating events based on the performance information gathered.

Additional information on Quest and the QMX is available on its website at http://www.quest.com/Quest_Management_Xtensions_for_MOM/.

Network Management Packs

Two vendors currently provide network-related management packs: eXc and Jalasoft (ordered alphabetically). Table 19.2 shows the vendors and network systems monitored. Both of these products enable MOM 2005 to monitor network devices.

TABLE 19.2 Vendor and Network Systems Monitored

Vendor	Hardware Device Monitored
eXc	Cisco, F5, 3Com, McData, NetApp, Nortel, and others
Jalasoft	Cisco, F5, HP Procurve, APC UPS, and others

eXc

eXc Software's network management packs for MOM 2005 use a Cisco virtual agent that leverages a custom WMI event provider to communicate with MOM. The eXc solution supports all SNMP-capable products for Cisco, F5, 3Com, McData, NetApp, Nortel, and other vendors. The eXc virtual agents are customizable. A free 30-day evaluation version of the eXc Cisco virtual agent and additional information about the eXc solutions are available at http://www.excsoftware.com/version3/version3/Products.aspx.

Jalasoft

Along with the non-Windows server management pack information provided earlier, Jalasoft provides network management packs for MOM 2005. The Jalasoft architecture is discussed in the "Non-Windows Server Management Packs" section earlier in this chapter and is also used with the Jalasoft network management products. The Jalasoft solution can monitor APC UPS, Cisco PIX Firewalls, Cisco Routers, Cisco Switches, Cisco VPN Concentrators, F5 BIG IP, HP Procurve Switches, and general network devices. A free 75-day evaluation version of the Jalasoft network management packs (which allows a user to run one NMS and discover up to 10 devices) and additional information is available from Jalasoft's website at www.jalasoft.com.

Third-Party Application Management Packs

A number of third-party vendors provide useful management packs for software applications. Although you should always look at Microsoft's Management Catalog for the current list of available management packs, we highlight a sprinkling of management packs in Table 19.3. The management packs are listed in alphabetical order by vendor.

TABLE 19.3 Vendor and Application Management Packs

Vendor	Application Monitored
Bindview	IT Security compliance across multiple platforms, applications, and databases.
Citrix	Monitors MetaFrame XP Enterprise Edition presentation servers and server farms.
eXc Software	Monitors and controls CheckPoint devices.
iVision	Blackberry Enterprise Server infrastructure and handheld devices.
Secure Vantage Technologies	Tracks auditing requirements for regulations such as the Sarbanes-Oxley Act, GLBA, HIPAA, and FISMA.
Tidal Software	Horizon for SAP manages incoming SAP system alerts.
Veritas (now Symantec)	Directs alerts from Veritas Backup Exe to on-call personnel. Additionally, the VERITAS Storage Foundation for Windows MP monitors events and performance counters generated by disks, disk groups, and volumes managed by its Storage Foundation product.

These are only a small sampling of the third-party solutions available. Check the Management Pack Catalog at http://go.microsoft.com/fwlink/?linkid=43970 for a complete list. The Product Connectors Catalog is maintained separately at http://www.microsoft.com/mom/downloads/momprodconnectors.mspx.

Solution Accelerators

MOM 2005 solution accelerators can also enhance Windows Server environments that use MOM 2005. As mentioned in Chapter 1, "Operations Management Basics," the solution accelerators offer ITIL-based best practices and prescriptive guidance for operational management processes and support the quadrants of the MOF process model. In plain English, this means the solution accelerators are a set of somewhat disparate tools that greatly enhance the functionality of MOM.

The MOF Process Quadrants

The quadrants of the MOF process model are Changing, Operating, Supporting, and Optimizing. An overview of the MOF process model and its quadrants is available at http://go.microsoft.com/fwlink/?linkid=50275.

The accelerators target two areas that correlate with several quadrants of the MOF process model:

- Alert management—The Operating quadrant focuses on performing day-to-day tasks efficiently and effectively, whereas the Supporting quadrant deals with resolving incidents, problems, and inquiries in a timely manner. By managing an incident during its life cycle, alert management becomes more effective. For example, you may elect to be informed only of alerts that would improve responses.
- Service continuity—The Optimizing quadrant includes availability in delivering IT services. In the event of a system failover, procedures should be in place for the outage to be virtually unnoticed by users. You can use MOM to implement best practices to recover from a MOM 2005 database failover, which would help protect data should a geographic or other disaster impact your implementation.

Six solution accelerators are currently available for MOM 2005. You can obtain this collection of tools at http://go.microsoft.com/fwlink/?linkid=46590, or as part of the MOM 2005 Resource Kit, which is available for download at http://go.microsoft.com/fwlink/?linkid=34629. Chapter 17 discusses the MOM SLA Scorecard for Exchange solution accelerator. This chapter describes the other five solution accelerators.

Using the Solution Accelerators

The solution accelerators are targeted for IT professionals in data centers and in large and enterprise organizations. Each solution accelerator requires preparation and planning. Many organizations choose to use consulting organizations experienced with these tools to assist with implementation.

Alert Tuning Solution

This tool helps fine-tune management packs before deploying them to production. It can reduce the initial volume of alerts by filtering out noncritical or unimportant alerts. The solution also provides prescriptive guidance to address alert noise reduction. Alert overload or "noise" can cause operators to spend time navigating through insignificant alerts and lead to operational ineffectiveness—caused by delays in response to legitimate alerts.

The Alert Tuning Solution Accelerator consists of documentation to guide you on the installation and usage of the accelerator (Optimizing MOM 2005 Alert Volume.doc), a test plan, and test plan details. The solution accelerator also includes reports to assist you with identifying where high levels of alerting are occurring within your MOM environment.

Figure 19.15 shows the alert count per week for the Microsoft Operations Manager Management Pack. Note that the report does not have an option available to report on all management packs; you must choose a single management pack for the report. This report provides a way to identify trends in alerting. In the example shown in Figure 19.15, it appears that alerts for this management pack peaked at the end of April.

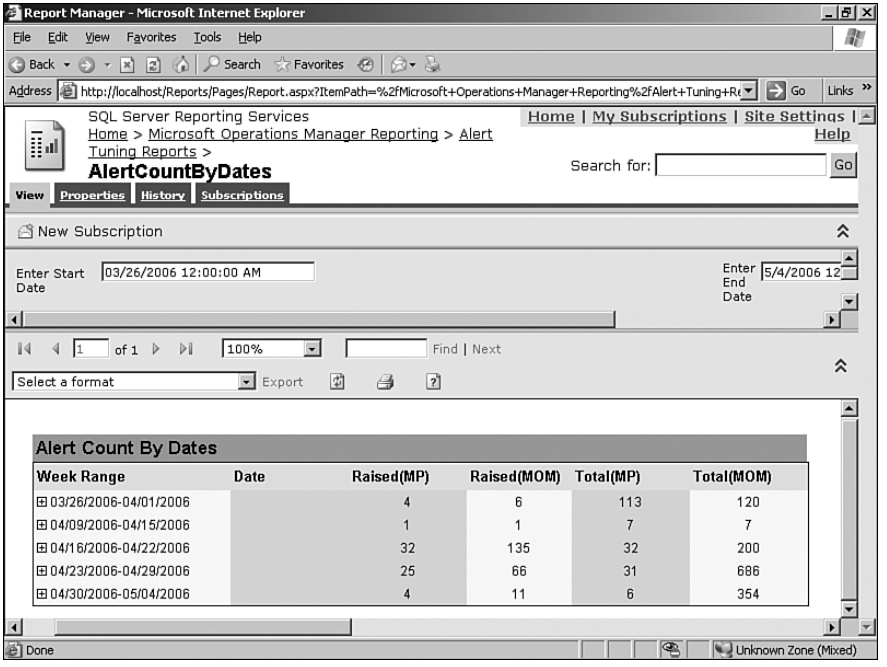


FIGURE 19.15 Alert counts by week for the MOM Management Pack.

Figure 19.16 shows the alert count per device (system) within a date range specified for a computer group. To run this report you need to specify a management pack, date range, and computer group. In this example, the number of alerts raised was close between the two systems, but the total number of alerts was much higher on Monarch (most likely due to suppressing duplicate alerts).

Figure 19.17 displays the number of raised alerts and total alerts by the processing rule that generated them. To run this report, specify a management pack, date range, and computer group. This is our personal favorite of the reports because it gives a quick insight into specific rules that are generating high levels of alerts.

Installing the Reports for Alert Tuning

Unlike most reports that are added into MOM by importing them into the MOM Administrator console, a different process is required to install the Alert Tuning reports. After installing the alert_tuning.msi, a second installation is required for the actual reports. The Alert Tuning Reports.msi extracts files required for the reports (by default saved to %*ProgramFiles*%\Microsoft\Alert Tuning Reports) and does some initial configuration but does not install the reports. To run the MSI specify the MOM servername, MOM database name, and the MOM database instance. After completing the installation, you must take additional steps to create the reports:

1. Open the Reporting console under the Microsoft Operations Manager Reporting folder and create a new folder called Alert Tuning Reports.

2. Within this folder you import three RDL files separately (alertcountbydates, alertcountbydevice, alertcountbyprocessingrules) and then create a OnePoint data source.
3. Link the reports to the new data source that you created.

Additional information is available in the management pack guide available with the documentation included in the Alert Tuning solution accelerator download.

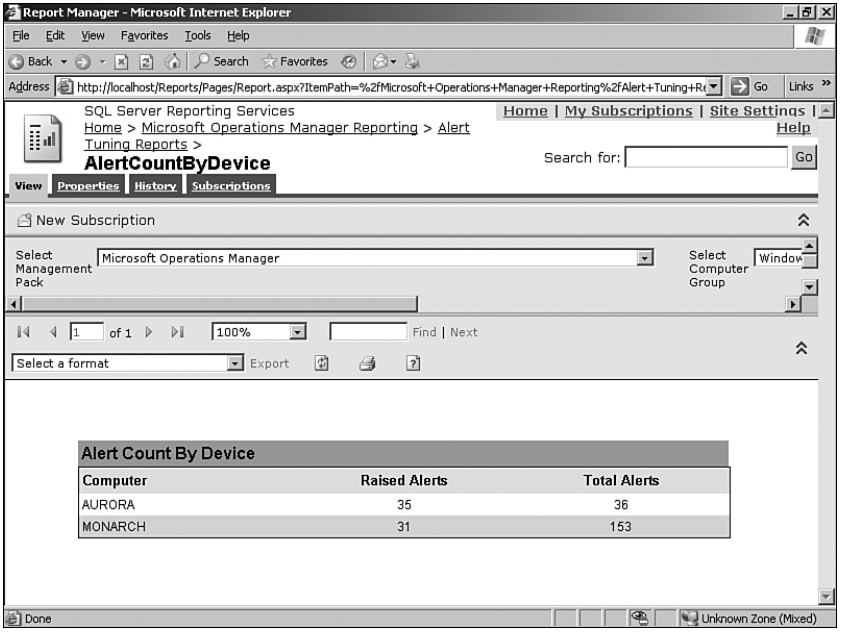


FIGURE 19.16 Alert counts raised and total by system.

The Alert Tuning solution can assist you in tuning your MOM environment. Additional documentation regarding the Alert Tuning Solution Accelerator is available at http://go.microsoft.com/fwlink/?linkid=46629.

Autoticketing Solution

To improve the efficiency of your help desk, the Autoticketing Solution Accelerator supports automated ticket generation, which enables automated posting of a request (ticket) into a sample Trouble Ticketing (TT) system used for incident management. Using autotickets, the solution accelerator facilitates quicker and more effective responses to service incidents and improves accuracy and speed when receiving information.

The autoticketing workflow diagram shown in Figure 19.18 includes nine steps describing the workflow occurring when MOM uses the autoticketing solution accelerator:

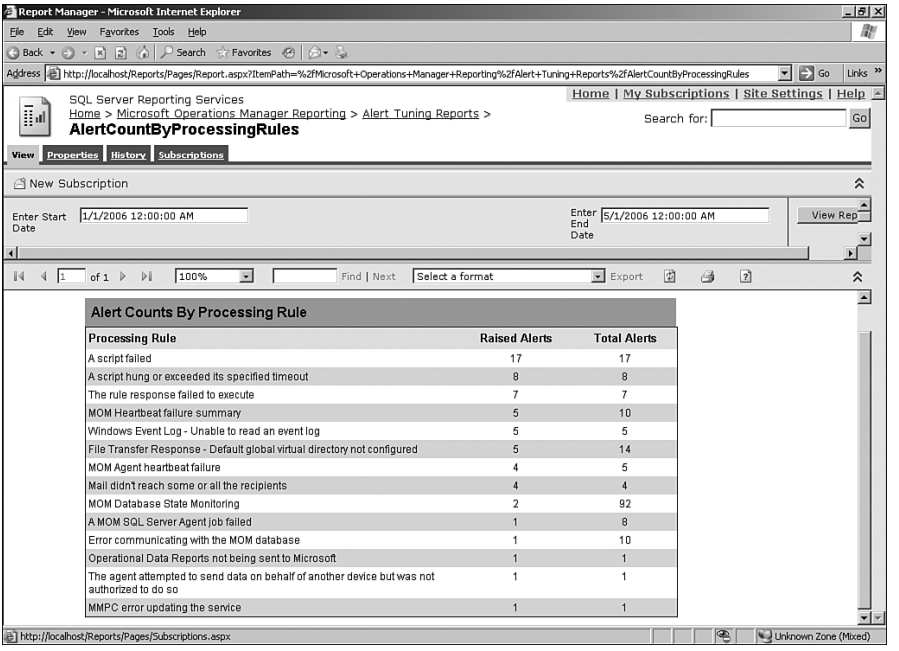


FIGURE 19.17 Alert counts by processing rule.

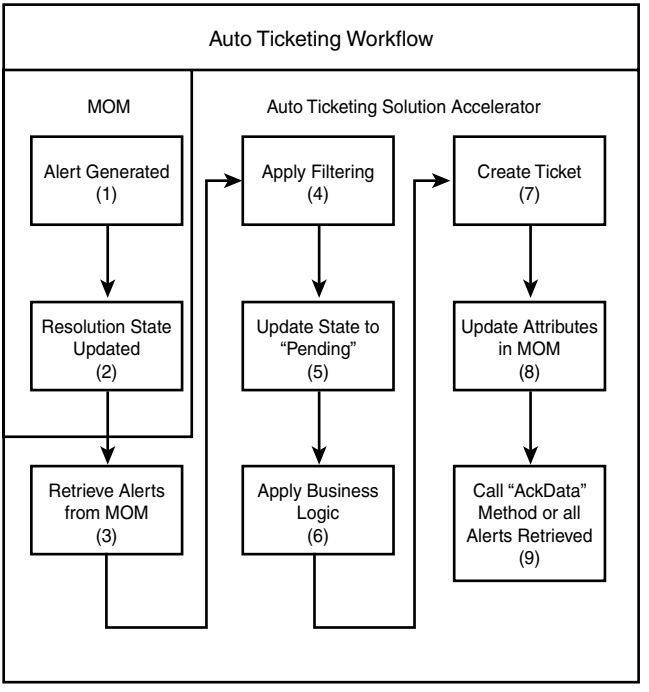


FIGURE 19.18 Autoticketing workflow.

1. First, MOM generates an alert.
2. A resolution state is defined for the alert (for more details on resolution states see Chapter 14). The alert automatically creates a ticket if the resolution state is configured to be AutoTicket, where AutoTicket is a resolution state type created by this solution accelerator.
3. Using the MCF, the autoticketing workflow retrieves alerts from MOM that have the resolution state set to AutoTicket.
4. Filtering is applied using business logic to determine whether the alert meets specific criteria or other system conditions.
5. The MCF is used to set the resolution state to Pending instead of the default state of New.
6. Business logic is applied to resolve data issues so that the ticket information is complete.
7. A ticket is created in the Trouble Ticket system.
8. After the ticket is created, attributes in the MOM alert are updated to reflect this new state and other information.
9. The AckData method is called to acknowledge that the workflow is completed.

The Autoticketing Solution Accelerator contains a document (Automatic Trouble Ticket Generation Using MOM 2005.doc) to help you prepare for and implement autoticketing and includes the workflow process just discussed. This solution accelerator offers increased operational efficiency by

- Reducing or preventing service incidents with proactive remedial action
- Faster and more effective responses to service incidents
- Improved overall availability of services.

The Autoticketing Solution Accelerator is documented at http://go.microsoft.com/fwlink/?linkid=50277.

Multiple Management Group Rollup Solution

Without customization, MOM 2005 is designed to transfer data from a single OnePoint database to one data warehouse. This solution works well when you are using a single management group, but with multiple management groups and multiple databases, it would be nice to have a single aggregation of the data. The Multiple Management Group Rollup Solution Accelerator enables an organization to aggregate data from multiple management groups into a central data warehouse for consolidation and reporting.

Installing MOM Reporting creates a single Data Transformation Services (DTS) package that is called by an executable program within a scheduled task. This DTS package runs

on the data warehouse server and pulls data from the management group into the data warehouse. Additional scheduled tasks are required to provide data transfer from multiple management groups to a single data warehouse. The accelerator gives guidance for creating these scheduled tasks and configuring them to specify additional management groups.

Figure 19.19 shows an example of how multiple management groups can be rolled into a single data warehouse. In this example the Contoso_Admin management group has a SQL Server cluster named Evergreen that uses DTS to write to the MOM reporting database on the Ridgeway cluster. The Contoso_Security management group is running on a single server (FortCollins) and also uses DTS to write to the MOM reporting database on the Ridgeway cluster. Both DTS packages run at different times to avoid contention (recommended by the solution accelerator documentation).

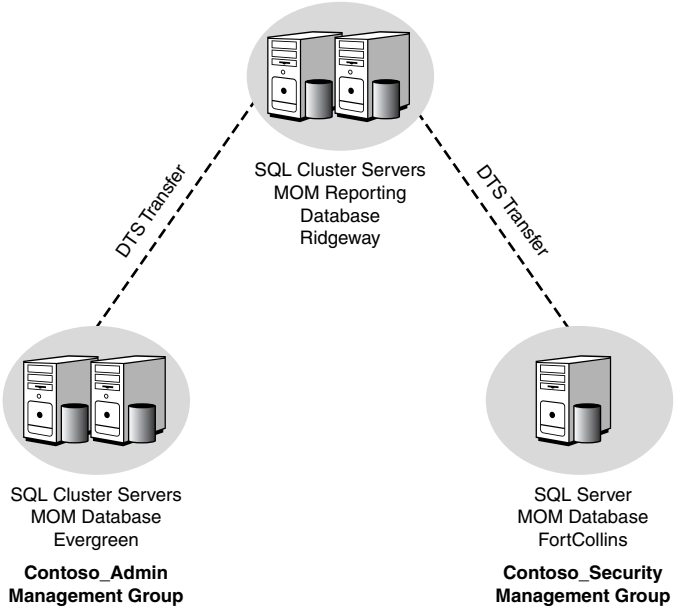


FIGURE 19.19 Multiple Management Group Rollup.

The rollup accelerator provides the ability to

- Store long-term operational data from multiple MOM 2005 management groups
- Develop reports providing information to analyze overall infrastructure reliability, capability, and behavior

Known Issues with the Multiple Management Group Rollup Solution Accelerator

Three reports are known to have problems rolling up multiple management groups into a single data warehouse:

- Operational Data Reporting \ Management Group Health—Only one management group is displayed in the report.
- Operational Health Analysis \ Alert Analysis—The report results are invalid because alerts appear multiple times in the report.
- Microsoft Operations Manager \ Agent Health Detail—The report results are invalid because alerts appear multiple times in the report.

The Management Group Rollup Solution Accelerator provides guidance on using multiple DTS packages to write to the same MOM reporting database. The solution accelerator consists of a test execution report, a test plan, and test case details. The Multiple Management Group Rollup Solution Accelerator is documented at http://go.microsoft.com/fwlink/?linkid=50279.

Notification Workflow

The Notification Workflow solution can target alerts to a particular individual responsible for managing a group of servers. At this time, the software is an SQL Server 2000-based Notification Services application that extends the existing notification capabilities in MOM 2005 (see http://support.microsoft.com/kb/922342/ regarding SQL Server version support for this solution accelerator). It allows a user to subscribe to, and be notified when, alerts associated with specific applications or services are generated.

No Escalation Capabilities

There had been discussion about providing functionality around escalation as part of the Notification Workflow Solution Accelerator. The most recent update for the solution accelerator does not include escalation capabilities, and it appears that the functionality is no longer planned. For additional information on escalation, see Chapter 14.

When a match for an alert occurs, an alert notification is sent to the subscriber. Subscribers and their schedules can be configured from the Subscriber Schedules tab of the Notification Workflow website. Figure 19.20 shows the schedule for a 24x7 administrator with one hour booked as a schedule override.

Notifications can be sent based on the subscriber's scheduling and extended MOM alert properties. These alert properties include computer name, alert source, alert severity, management pack name, computer group name, device, and alert description as shown in Figure 19.21.

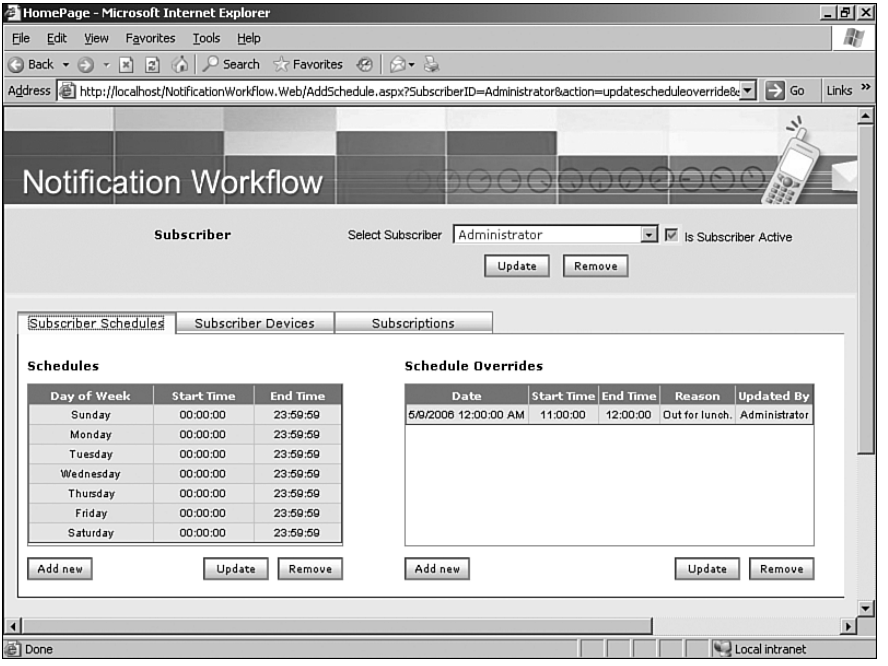


FIGURE 19.20 Fields available when creating a subscription.

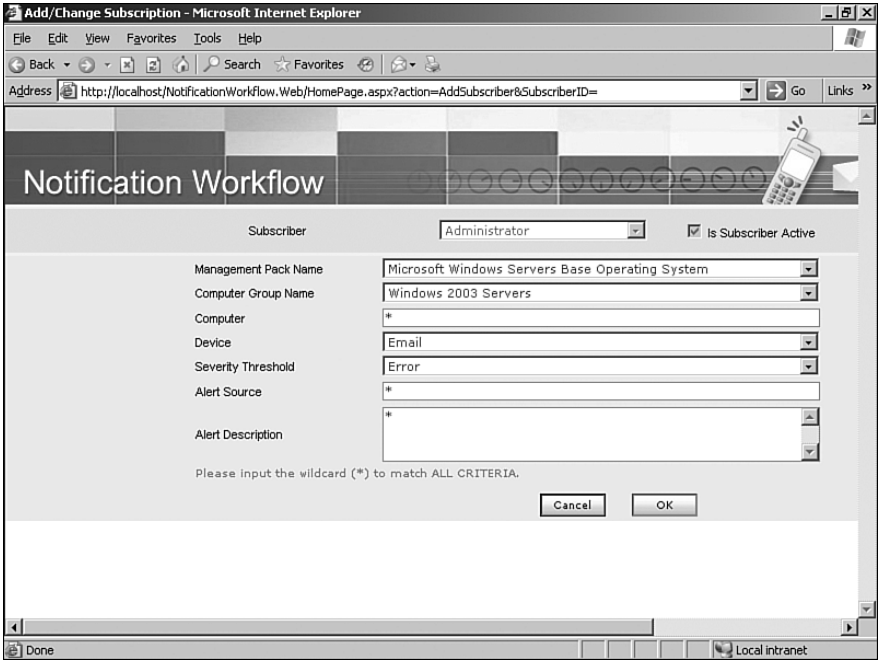


FIGURE 19.21 Creating a subscription within the Notification Workflow solution accelerator.

The solution accelerator includes an installation guide, user guide, test plan, test case details, and code. The user guide may be accessed directly at http://go.microsoft.com/fwlink/?linkid=50278.

Implementing the Notification Workflow Application

Several known issues with the Notification Workflow application are documented in the Notification Workflow User Guide. Check the Microsoft Knowledge Base at http://support.microsoft.com/kb/894486/ for additional information. Additionally, the solution accelerator is not supported on an SQL Server 2000 cluster (http://support.microsoft.com/kb/917666/).

Service Continuity Solution

Because an operations management tool monitors the availability of business services and applications, it is important that MOM maintain high levels of availability and continuity. The Service Continuity Solution Accelerator is a process to implement disaster recovery for MOM 2005, and includes best practice guidance and automation tools to help minimize the downtime in the event of an infrastructure failure.

The Service Continuity Solution Accelerator provides direction on creating a DTS package to transfer data from an existing MOM OnePoint database to a backup OnePoint database located in a disaster recovery location. The DTS package can then be called to synchronize the primary database and the failover database for that management group. If there is a requirement to transfer operations to the disaster recovery location MOM can either be manually "repointed" to the new database or automatically transferred using a script available with the solution accelerator.

Figure 19.22 shows an example of how this solution accelerator could be used in a sample environment. The Frisco site has a production SQL Server cluster named Evergreen, which provides the production database for the Contoso_Admin management group. The Houston site is the company's disaster recovery location and is connected to the Frisco site by a WAN link. The Houston site has a server named Durango that is synchronized with the Evergreen cluster using the DTS package using the information provided within the Service Continuity Solution Accelerator.

The MOM 2005 Service Continuity Solution provides the capability for the following:

- Increased availability and continuity of monitoring services within Information Technology (IT) operations
- Automation for rapid failover of the MOM 2005 service
- Various architectural configurations spanning multiple geographical locations
- Application of IT Infrastructure Library (ITIL) and Microsoft Operations Framework (MOF) IT processes into the organization

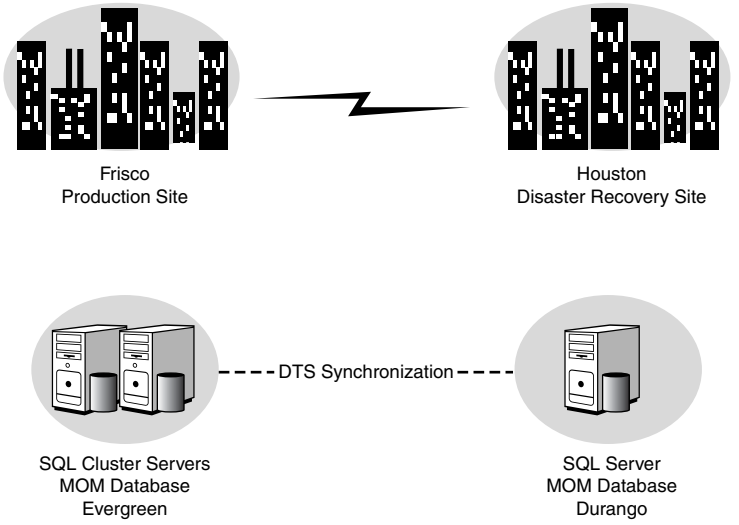


FIGURE 19.22 Service Continuity diagram.

The solution accelerator consists of an installation guide (Establishing MOM 2005 Service Continuity.doc), a sample DTS package, a test plan, and test case details. Further information on the Service Continuity Solution is available at http://go.microsoft.com/fwlink/?linkid=50276.

Summary

This chapter focused on how to extend MOM's interoperability with other systems by providing information for using the MOM Connector Framework, options offered by third-party vendors, and information on the Microsoft solution accelerators. In the next chapter we will discuss approaches to create your own management packs to further increase the capabilities of your MOM environment.

CHAPTER 20

Developing Management Packs

IN THIS CHAPTER

- Developing Management Packs
- Using the Management Pack Wizard
- SecurityPack Management Pack
- PingPack Management Pack
- Next Steps for the PingPack

In Chapter 19, "Interoperability," we demonstrated Microsoft Operations Manager (MOM) 2005's capabilities to communicate with other systems by using product connectors, solution accelerators, and various third-party management packs. Now we will discuss another aspect of increasing MOM's functionality: creating your own management packs! The main topics we will cover are developing management packs and using the Management Pack Wizard to facilitate the management pack creation process. Our discussion will only cover the basics of management pack development by presenting the steps required to create simple management packs; an entire book could be devoted to the creation of sophisticated management packs.

Developing Management Packs

To assist in the process of developing management packs, Microsoft provides the Management Pack Wizard tool in the MOM 2005 Resource Kit. The Management Pack Wizard guides the user in creating rule groups and relationships with computer groups as part of building a complete management pack.

This chapter walks through the management pack design and development process while addressing possible solutions to common MOM requests. The following key areas will be reviewed in detail: the first area covers the functionality associated with the Management Pack Wizard and then we will focus to how to manually build a management pack:

- Management Pack Wizard—This section walks through the process necessary to create a new management pack using the Management Pack Wizard.
- SecurityPack—Walks through the creation of a Windows security event monitoring management pack, a common request from many organizations that have already implemented or are thinking about implementing a MOM monitoring solution.
- PingPack and network system monitoring—Covers another common request, the ability to "ping" network devices and respond when the device is unavailable. Devices can include routers, firewalls, or anything else that responds to a ping.

These examples provide the foundation necessary to build additional custom management packs both with and without the Management Pack Wizard. Each section covers the steps necessary to design and configure the various elements of a custom management pack, from the business logic within the rule groups that define how the management pack will monitor the target system, to the Operator console views that allow the data to be effectively displayed and utilized.

How Rules Are Applied to Computers

Before jumping into the design process, it is important to understand how rules in the rule groups are applied to the correct target computers. This process, shown in Figure 20.1, starts after the MOM agent is deployed. The agent downloads the list of attribute definitions from the management server and performs a local scan, the results of which are sent to the management server. The attribute scan results allow the management server to dynamically add or remove the computer from the various computer groups. As rule groups are linked to computer groups, when a computer is added to a computer group the rules linked to that group are automatically applied. In the same way, when a computer is removed from a computer group the linked rules are automatically removed.

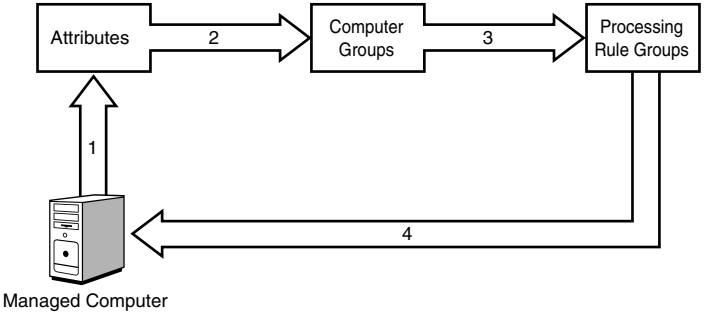


FIGURE 20.1 How rules are applied to computers.

Figure 20.1 includes the following components:

- Attributes—Attribute definitions are part of management packs. Attributes simply define registry key locations on the target system that will be checked during the

attribute scan process. By default, this scan takes place every 60 minutes but can be configured within the global settings of the Administrator console.

- Computer groups—Computer groups can be static or dynamic. Dynamic computer groups use search criteria to find potential group members and formulas to check attribute values to filter the search results.
- Rules—Rule groups are linked to computer groups. Members within a linked computer group download the rules that define how the system will be managed.

Technicalities in Terms

It is common to refer to the process of "applying" or "deploying" rules to computers. It is important to remember that this term refers to the assignment of rules to a group of MOM agents. All agent communication is initiated from the client; the process of "applying" rules allows the agent to download the rules during the next polling cycle. The management server never actually "pushes" these settings down to an agent.

Designing a Management Pack

When you decide that it is necessary to create a custom management pack, consider the business logic along with the functionality that best supports the business.

For our SecurityPack Management Pack, we want to collect information such as various parameters from each of the security events that may be considered important. Gathering this dictates creating "collection" event rules. Collection event rules have the capability to store each of the parameters associated with an event, which is helpful when building reports because these parameters can be easily searched. For example, if we create a rule to collect the security event and corresponding parameters associated with "account creation," an interactive report could easily be created that would search the various parameters to find key information, such the person who created the account and the name of the account that was created.

However, collection events have some functional limitations, primarily that they do not generate alerts. If people in your organization would like real-time alerts when specific security events are generated, alert event rules are required. An alert rule generates a notification as a response to a predefined condition, such as a specific security event on a server. It is acceptable to create both collection and alert rules for the same event, for example, on security events that need to send a notification and will be used in reports.

In the PingPack Management Pack we want to extend the base functionality of MOM through a custom script; this would dictate the creation of "timed" event rules. The timed event rule performs a custom action against target computers. This timed event rule will be configured to launch the PingPack Visual Basic script at a predefined interval to test a list of network devices. This management pack also implements state alerts that update the State view of a device. For example, if a monitored device becomes unavailable, the State view indicator changes from green to red, and then back to green when the device

becomes available. Chapter 22, "Using and Developing Scripts," discusses additional tips and tricks and provides a look into creating scripts and managed code assemblies capable of interacting with the MOM environment.

Using the Management Pack Wizard

The Microsoft Management Pack Wizard is a utility that creates management packs. The Management Pack Wizard is part of the MOM 2005 Resource Kit (http://go.microsoft.com/fwlink/?linkid=34629). This wizard must run on a MOM 2005 management server. The wizard provides an easy-to-use interface for building a management pack, which can include rule groups, services to monitor, performance thresholds, and event monitoring. The wizard can also generate scripts and underlying logic.

To use the Management Pack Wizard, install the MOM 2005 Resource Kit on the management server you will use to run the wizard. If you attempt to run this tool on a system that is not a management server you will receive the message displayed in Figure 20.2.

FIGURE 20.2 Error running Management Pack Wizard on a non-Management Server.

Let's take a simple example of what the Management Pack Wizard can do. Microsoft introduced Active Directory Application Mode (ADAM for short) with Windows 2003. ADAM is downloadable from Microsoft's website at http://go.microsoft.com/fwlink/?linkid=29359 and provides a Lightweight Directory Access Protocol (LDAP) directory that runs as a user service. For purposes of illustration, we installed ADAM on a MOM 2005 management server and used the Management Pack Wizard to create a simple management pack to monitor the service created by the ADAM installation.

The ADAM installation adds an event log, a service, and various performance counters to the system. In our example we will monitor the LDAP service (which we named Fabrikam) and the performance counters added from installing ADAM. To create this management pack using the Management Pack Wizard we go through the following steps:

1. Run the Management Pack Wizard, and on the Welcome screen shown in Figure 20.3 select the following options: Windows Service Monitoring and Performance Threshold Monitoring. We will leave Event Source Monitoring unchecked and click Next to continue.
2. On the Role Name screen enter the name **Fabrikam** for the Role Name and **Fabrikam ADAM** for the description.
3. On the Components screen we add Services and Performance as illustrated in Figure 20.4.

FIGURE 20.3 MOM 2005 Management Pack Wizard Welcome screen.

FIGURE 20.4 MOM 2005 Management Pack Wizard components.

4. On the Windows Service Monitoring screen, add the Fabrikam service (installed by ADAM), as displayed in Figure 20.5.

5. At the Performance Threshold panel, add the AD/AM NTLM Authentication performance object specifying a red threshold greater than 1000, as shown in Figure 20.6. We are specifying here that if more than 1,000 NTLM authentications per second occur within the Fabrikam ADAM, we will show the state as red. You would want to adjust this based on how many users are actually authenticating to the Fabrikam ADAM.

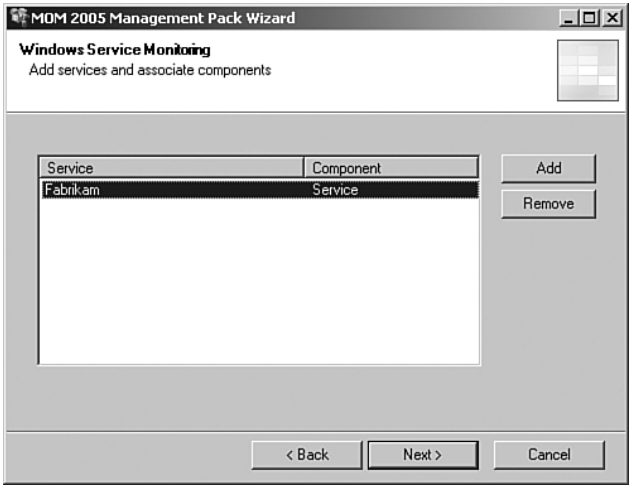


FIGURE 20.5 MOM 2005 Management Pack Wizard Windows Service Monitoring.

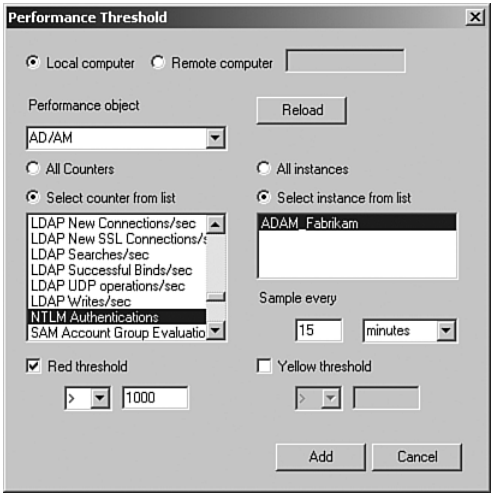


FIGURE 20.6 MOM 2005 Management Pack Wizard Performance Threshold Monitoring.

6. The wizard Summary screen displays a summary of your selections. Click Finish to build the management pack, and the wizard generates an akm file named fabrikam.akm located in the *%ProgramFiles%*\Microsoft Operations Manager Resource Kit\Tools\Management Pack Wizard directory.

7. Import the akm file into MOM 2005, using the procedure discussed in Chapter 13, "Administering Management Packs." Figure 20.7 shows the changes in the Administrator console after importing the akm. You will now see the addition of the Fabrikam rule group, which includes two event rules and one performance rule.

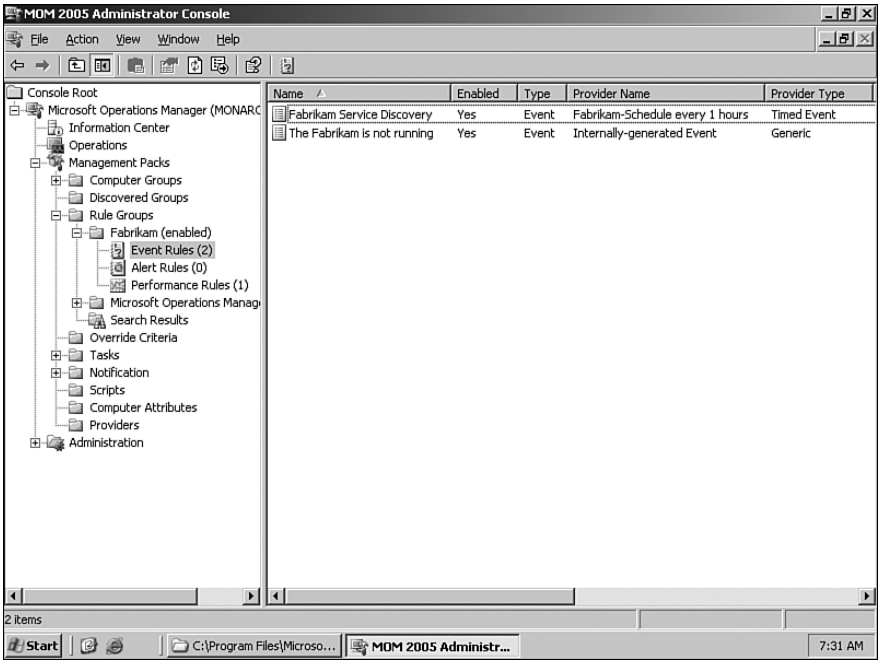


FIGURE 20.7 Fabrikam rule group added by the wizard.

Create a computer group for the system or systems that will be monitored by this management pack and associate this computer group to the rule group. More details on how to create this group and associate a computer group are discussed in the SecurityPack Management Pack example which follows this section.

9. Commit the configuration changes to apply them to the system referenced in the computer group.

The Event Source Monitoring feature of the Management Pack Wizard is also helpful. This option provides the ability to read all the events from a particular source. For example, if we were monitoring events generated by a third-party application, the event numbers may not be documented or widely available. In this case we can use the Management Pack Wizard's Event Source Monitoring feature to look into the corresponding event source DLLs on the target system and list every possible event. We can then choose the events we wanted to include in our management pack or simply import all the events available.

As discussed in this section, the Management Pack Wizard provides a quick and effective method to create simple management packs and can provide a starting point for more complex management packs.

SecurityPack Management Pack

It is common for MOM to be used to monitor security events on key managed computers such as domain controllers or special access systems such as accounting servers. Before creating a management pack that monitors security events, you will need to determine the monitoring scope. Considering the potential volume of security events that can be produced, a focused scope for security monitoring is important. For demonstration purposes, a security management pack will be created with the following objectives:

- Account logon activity—Monitor the number of attempts made when a user attempts to log on with an incorrect password or with a disabled account. When a specific number of failed attempts is made, an alert should be sent to the Security Admins group.
- Security group management—Monitor administrative group membership. When a user is added or removed from a predefined list of administrative groups an alert should be sent to the Security Admins group. Administrative groups will include Domain Admins, Enterprise Admins, and Schema Admins.
- User account management—Monitors user account management. Collects events associated with all user account management for the purpose of creating reports. Also monitors and alerts the Security Admins group when an account lockout occurs.

The list of security events within our management pack scope is generated on domain controllers; as such the security management pack will only be associated with domain controllers throughout the environment.

Creating a Rule Group

The security management pack development process starts with creating rule groups; these rules groups will ultimately hold the rules that define how the management pack monitors target computers. After determining the scope of the management pack, you can design an efficient rule group structure to manage the various rules. The security management pack we will create focuses on collecting events and alerting or responding to events on domain controllers throughout our environment. The scope of the security management pack can be divided into the following three categories; these categories can then be used to design our rule group hierarchy:

- Account Logon Activity
- Security Group Management
- User Account Management

Rule groups will be created for each of the three security categories. For organizational purposes, these rule groups will be placed inside a top-level rule group. The following steps can be used to create the top-level rule group:

1. In the Administrator console, navigate to Management Packs \ Rule Groups. Right-click on Rule Groups and select Create Rule Group.
2. On the General page, enter **Security Event Monitoring** in the Name field and enter a description such as, **Monitor security event logs on Windows servers** in the Description field. Click Next.
3. On the Knowledge Base screen, click Edit and enter information to describe the function of the SecurityPack. Figure 20.8 shows sample content describing what the management pack does and some of the Windows Security auditing prerequisites.

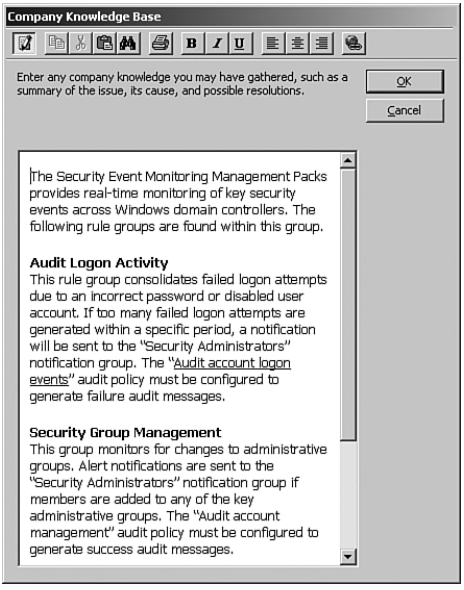


FIGURE 20.8 SecurityPack Knowledge Base.

4. Click Finish to complete the creation of the rule group, and click No when prompted to deploy the rules in this newly created rule group to a group of computers.

The Security Event Monitoring rule group is the top-level group in our rule group hierarchy. This group will not contain any rules; it will only contain lower-level rule groups and is used primarily for organizational purposes. Perform the following steps to create the remaining lower-level rule groups within the Security Event Monitoring rule group.

1. In the Administrator console, navigate to Management Packs \ Rule Groups, right-click Security Event Monitoring, and select Create Rule Group.
2. On the General page, enter **Account Logon Activity** in the Name field and enter a description, such as **Monitor account logon security events on Windows servers** in the Description field. Click Next.

3. On the Knowledge Base screen, click Edit and enter information to describe the function of this rule group. For example, you can include the intended purpose of this rule group along with the security audit settings required on each target system.
4. Click Finish to complete the creation of the rule group, click No when prompted to deploy the rules in this newly created rule group to a group of computers.

Repeat these steps to add the remaining two lower-level rule groups to the Security Event Monitoring rule group. These groups are Security Group Management and User Account Management. When finished, your rule group hierarchy for the Security Management Pack should look similar to Figure 20.9.

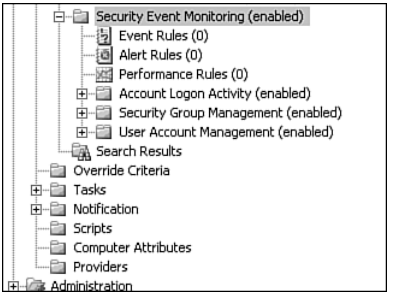


FIGURE 20.9 SecurityPack rule groups.

Creating a Computer Group

Computer groups allow you to apply a set of rules to a group of computers meeting a specific criteria. If you have already imported some of Microsoft's standard management packs, you will notice many computer groups already exist. You can use these rule groups if they target the same set of computers you have identified for the security management pack. For example, the rules in this management pack will be associated with domain controllers. If you are managing Active Directory and have already imported the Active Directory management pack, the computer groups for Windows 2000 Domain Controllers and Window Server 2003 Domain Controllers already exist. You can simply associate your security management pack rules with these existing groups. However, some important drawbacks should be considered when using groups from another management pack. The primary drawback is that you don't control these groups, and should Microsoft change these groups in the next release of the Active Directory management pack, any custom management packs that depend on those groups may be negatively affected. To play it safe, we recommend defining your own custom computer groups over which you can maintain complete control.

The following process can be used to create a custom computer group that will identify domain controllers in your environment:

1. In the Administrator console, navigate to Management Packs \ Computer Groups. Right-click on Computer Groups and select Create Computer Group. Click Next on the Welcome screen to begin.
2. On the General screen, enter the name **Security Event Monitoring - Audited Servers** and a description of servers you plan to include in the group.
3. On the Included Subgroups screen, accept the default setting to prevent any groups from becoming nested within this group. Click Next.
4. On the Included Computers screen, add the domain controllers you want to monitor by clicking the Add button and selecting the domain controllers from the list. The selected computers need to have the MOM agent installed. Click Next.
5. On the Excluded Computers screen, accept the defaults to prevent any computers from becoming explicitly excluded from the group. Click Next.
6. On the Search for Computers screen, accept the default Do Not Search for Computers option. This prevents the computer group from searching for members. Click Next.
7. On the Formula screen, accept the default Do Not Use a Formula to Determine Membership for This Computer Group option. This option is only necessary when the search options are configured. Click Next.
8. On the State Roll-up Policy screen, take the default value of The Worst State of Any Member Computer or Subgroup. This option indicates that the state of the entire computer group is equal to the most severe state of any member of the computer group. Click Next.
9. On the Confirm Choices screen, verify your specifications and then click Next. Click Finish to complete the Computer Group Wizard.

Searching for Computer Group Members

In the previous set of steps, a static list of computers was added to the computer group. For most environments a static list of computers significantly increases administrative overhead because changes to the environment such as adding, removing, or replacing monitored servers have to be manually replicated in any statically configured computer group. To eliminate this type of overhead, dynamic computer groups can be created. A dynamic computer group automatically finds the correct group members based on the specific criteria.

The objectives for the security management pack are to monitor for specific security events on domain controllers. Ideally, as new domain controllers are added, they should be automatically monitored by the security management pack.

The search properties for the computer group can be configured to automatically find all agents running on domain controllers. The following process can be used to access and configure the search properties of the computer group:

1. In the Administrator console, navigate to Management Packs \ Computer Groups. Right-click on the Security Event Monitoring - Audited Servers computer group and select Properties.
2. Select the Search for Computers tab, configure the properties of the tab to only search for domain controllers regardless of name. Figure 20.10 shows an example of the required configuration.
3. The static list of servers can now be removed by selecting the Included Computer tab and removing each of the computers shown in the list. Click OK to complete the configuration.

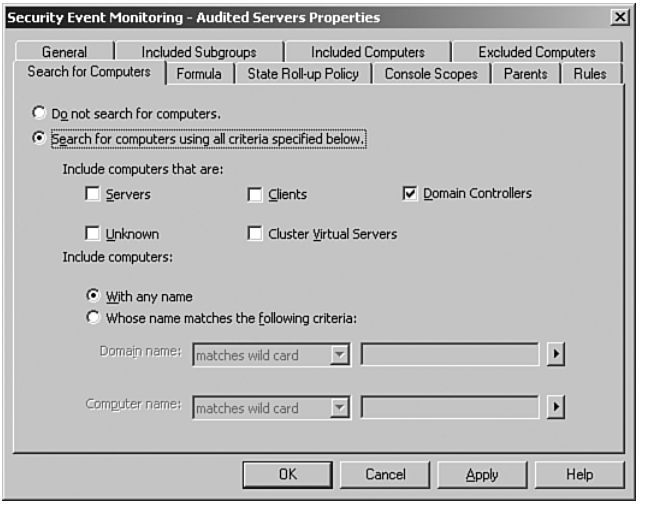


FIGURE 20.10 Search for domain controllers with any name.

Searching for Domain Controllers

The field that defines the "type" of server is never updated. For example, if you install a MOM agent on a member server and then promote the server to act as a domain controller, the computer group search function will never identify this system as a domain controller unless you completely remove the agent, delete the server object, and then reinstall the agent. In a real-world environment, you should configure dynamic computer groups based on formulas; this is discussed in the following section.

The Search for Computers tab provides a range of options including the ability to search by server type, such as domain controllers or virtual servers, in conjunction with name filtering including various wild cards, or regular expression pattern matching.

Using Formulas to Filter Search Results

In some cases, you may find the Search for Computers tab does not offer the flexibility needed to easily identify a group of servers in your environment. For example, you may want to monitor only domain controllers in a specific site because of the various boundaries or environmental conditions that may exist within your organization. In this case, you can complement the search with a formula. Although the Formula tab offers advanced filtering of the search results configured on the Search for Computer tab, this advanced filtering is based on attributes.

Attributes are registry values that are scanned periodically on all agents. The results of the attributes can then be used to provide advanced filtering of computer group search results. For example, applications installed on client computers can be identified by searching for specific keys in the registry. A formula in a computer group would then be configured to include computers that have these specific keys or a specific value within the key.

Attribute Scanning

The agent scans attributes every 60 minutes by default. This setting can be configured in the MOM Administrator console under Administration \ Global Settings \ Management Servers on the Discovery tab.

We will demonstrate how to use attributes by specifying that only domain controllers in a specific Active Directory site should be monitored. You would create the following attributes to look for the Active Directory site name in the registry:

1. In the Administrator console, navigate to Management Packs \ Computer Attributes. Right-click Computer Attributes and select Create New Attribute.
2. On the Type screen, select the Registry value option. Click Next.
3. On the Registry Path screen, browse to the following registry location on the local computer. This key holds the name of the current Active Directory site and is found on both domain controllers and member servers. Click Next.

   ```
   SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\Site-Name
   ```

4. On the Value screen, select Retrieve Registry Value and Convert to String. Click Next.
5. Enter a name for the attribute such as **Active Directory Site Name** and a description such as **Collects the name of the current Active Directory site**. Click Finish.

Finding the Active Directory Site Name

Normally the following key would be used to identify the AD site: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\DynamicSiteName. Although this key is updated faster than the one defined in the Active Directory Site Name attribute, it is not available on domain controllers.

Within 60 minutes MOM agents will perform a scan with the newly created attribute definition; the results of the scan will be viewable within the Operator console. To view the attributes found on each computer, do the following:

1. In the Operator console, select Public Views; then select the Computers node from the menu tree.
2. The Computer Details pane shows all the attributes that have been identified on the selected computer. Figure 20.11 shows the Attributes tab. The Active Directory Site Name attribute contains the value Site-01; this corresponds to the Active Directory site the server is located in.

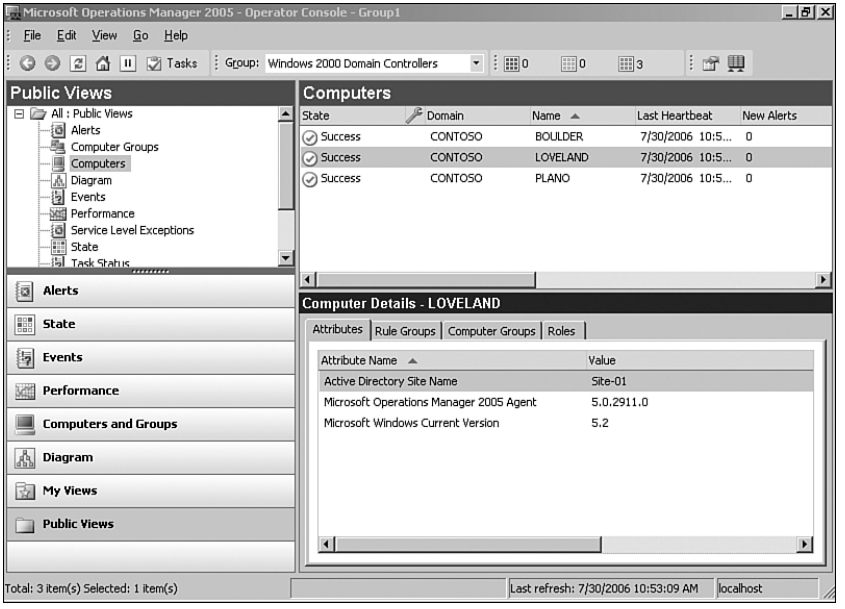


FIGURE 20.11 Active Directory Site Name within the Attributes tab of the Computer Details.

Manually Initiate an Attribute Scan

You can manually initiate an attribute scan within the Administrator console. Navigate to Administration \ Computers \ Agent-managed Computers. Right-click on one or more agents and select Run Attribute Discovery Now.

Now that the Active Directory site name is being collected and stored in the MOM database, a filter based on this name can be added to the Security Event Monitoring - Audited Servers computer group. To define the filter, do the following:

Monitoring for Security Events

The following is provided as an example only. Monitoring a limited number of domain controllers is a security risk. Unless you have a good reason, it is highly recommended to monitor security events on all domain controllers as to avoid inconsistencies.

1. In the Administrator console, navigate to Management Packs \ Computer Groups. Right-click on Security Event Monitoring - Audited Servers and select Properties.
2. Select the Formula tab and select Specify a Formula for the Computer Group.
3. Click the Attribute button and select the Active Directory Site Name attribute from the list. Click OK.
4. Select the Operator button and select the "=" sign; then following the equal sign type the name of the Active Directory site you want to include in your search. You should place the site name in quotes. Your formula should look similar to Figure 20.12. Click OK to complete the configuration.

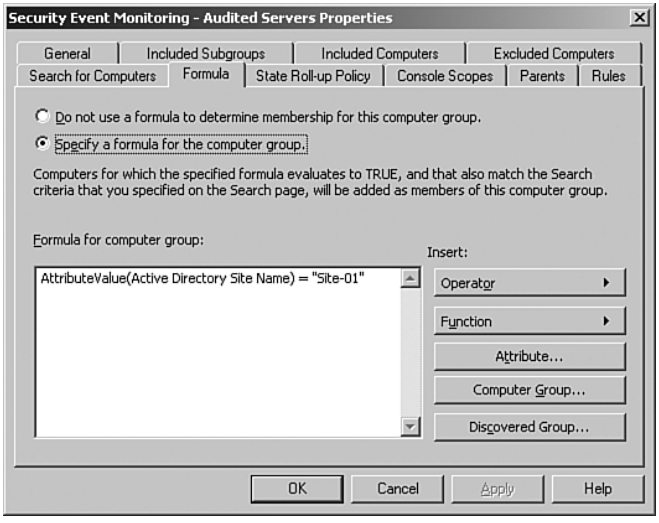


FIGURE 20.12 Active Directory Site formula.

As you can see by adding attributes, we can identify custom information about each MOM agent. Based on this data, computers can be automatically added to computer groups, which are associated with monitoring rules. This is an important step in lowering the administrative overhead of your MOM infrastructure. Our custom security rules are now being applied to domain controllers in a specific site.

Associate the Computer Group and the Rule Group

After creating the rule groups and the computer group, you will want to associate the computer group to the rule group. Associating a computer group to a rule group causes the rules to apply to the members of the computer group.

In this example we are linking the Security Management Pack rules to the Security Event Monitoring – Audited Servers computer group. To create the association, perform the following:

1. In the Administrator console, navigate to Management Packs \ Computer Groups. Right-click Security Event Monitoring and select Properties.
2. On the Computer Groups tab add the Security Event Monitoring – Audited Servers group, as shown in Figure 20.13. Click OK.

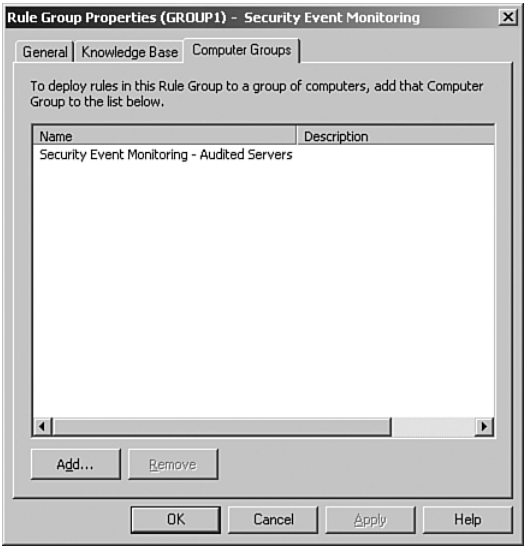


FIGURE 20.13 Rule group—computer group link.

Linking the top-level rule group, Security Event Monitoring, with a computer group automatically assigns all lower-level rule groups to the computer group as well. By default, changes to rule assignments are downloaded by agents once a minute. To manually initiate downloading rules, from within the Administrator console right-click Management Packs and select Commit Configuration Change.

Troubleshooting Your Management Packs

If you have created your own management pack and it doesn't seem to be generating any activity, verify that you have associated a computer group with a rule group in the management pack hierarchy. Without an association, the management pack will not be deployed to an agent.

Adding Rules to Your Rule Groups

After linking the computer and rule groups, you can add the rules that will facilitate collecting and responding to the various security alerts. Based on the security management pack objectives outlined at the beginning of the "SecurityPack Management Pack" section, we will be simply collecting and responding to generic windows security events. These events were tested within a Windows Server 2003 Active Directory domain, although most of these events are also compatible with a Windows 2000 Active Directory domain.

Several options exist to obtain the event numbers that correspond to our management objectives. Microsoft has documented some of the common security events in the Windows Server 2003 Security Guide. This guide is available from Microsoft's download site (http://www.microsoft.com/downloads); search for "Windows Server 2003 Security Guide." We can also set up a POC (proof of concept) environment to test and record the security events for the types of actions we want to monitor.

Finding Event Numbers

If we were monitoring events generated by a third-party application, the event numbers may not be documented or widely available. In this case we can use the Management Pack Wizard available in the MOM 2005 Resource Kit. The Management Pack Wizard looks into the corresponding event message DLLs on the target system and lists every possible event. This is helpful when developing management packs for third-party applications.

Creating Collection Rules

The monitoring objectives for this management pack are reasonably light; we can simply search for the events we like in the Windows Security Guide and then manually add them to the various rule groups in our management pack.

Starting in the Account Logon Activity rule group, use the following procedure to create the events listed in Table 20.1. Then create the events in Table 20.2 in the Security Group Management rule group, and finally create the events listed in Table 20.3 in the User Account Management rule group.

Use an Alert Template

After the first collection rule is correctly configured, you can simply right-click and then copy and paste a clone of the rule within the same rule group on to another rule group, each "copied" rule can then be updated with the correct name and event ID.

1. In the Administrator console, navigate to Management Packs \ Rule Groups \ Security Event Monitoring. Expand the corresponding rule subgroup for the rules you want to enter and select the Event Rules category.
2. Right-click on Event Rules and select Collect Specific Events.

3. On the Data Provider screen, select Security from the Provider Name drop-down. Click Next.
4. On the Criteria screen, enable the With Event ID check box and enter one of the event IDs from the following tables. For example, the first event ID in Table 20.1 is 675, so type **675** in the Event ID field.
5. Enable the Of Type check box and enter the correct Audit Type for the event as listed in the corresponding tables. Click Next.
6. On the Parameter Storage screen, select Store All Event Parameters; click Next.
7. On the Schedule screen, accept the default Always Process Data. Click Next.
8. On the Knowledge Base screen, feel free to enter some additional details about the type of event being collected. Click Next.
9. On the General screen, enter the correct name of the event as listed in the corresponding table. Click Finish.

TABLE 20.1 Account Logon Activity

Name	Audit Type	Alert Type	Event ID
Pre-authentication failed (incorrect) password)	Failure Audit	Collection	675
Authentication ticket request failed (disabled account)	Failure Audit	Collection	672

TABLE 20.2 Security Group Management

Name	Audit Type	Alert Type	Event ID
A member was added to a global group	Success Audit	Collection	632
A member was removed from a global group	Success Audit	Collection	633
A member was added to a local group	Success Audit	Collection	636
A member was removed from a local group	Success Audit	Collection	637
A member was added to a security-enabled universal group	Success Audit	Collection	660
A member was removed from a security-enabled universal group	Success Audit	Collection	661

TABLE 20.3 User Account Management

Name	Audit Type	Alert Type	Event ID
A user account was created	Success Audit	Collection	624
A user account was deleted	Success Audit	Collection	630
A user account was automatically locked	Success Audit	Collection	644
Account was unlocked (Active Directory 2003 Only)	Success Audit	Collection	671

The collection rules in each of the rule groups also facilitate the report development process by collecting individual parameters for each event. The next objective of the management pack is to alert security admins when something isn't quite right.

Creating Alert Rules

To notify operators/administrators of a problem, event rules can be created to alert or respond to a condition. It is important to note that the alert rules and the collection rules are independent, and each can exist on its own.

Alerts in the security management pack will be configured that correspond to the different objectives outlined at the beginning of the "SecurityPack Management Pack" section.

- A user account is locked out.
- A member is added to an Administrative group.
- More than 15 failed logons have occurred within 1 minute.

Before creating the alert rules, the correct notification group must be defined. To create the Security Administrators notification group, perform the following steps:

1. In the Administrator console, navigate to Management Packs \ Notification \ Notification Groups. Right-click Notification Groups and select Create Notification Group.
2. In the Name field enter **Security Administrators**. If the desired operators have already been created, add them to the group by moving the account from the Available Operators list to the Group Operators list. If those operators have not been created, click the New Operators button to define the operator settings.
3. Click Finish to complete the Notification Group configuration.

The first alert rule generates an alert each time a user account is locked out. This rule is simple in nature and can be created by doing the following:

1. In the Administrator console, navigate to Management Packs \ Rule Groups \ Security Event Monitoring \ User Account Management. Right-click Event Rules and select Alert on or Respond to Event.
2. On the Data Provider screen, select Security in the Provider Name list. Click Next.
3. On the Criteria screen, enable With Event ID and enter **644** in the field provided. Enable Of Type and select Success Audit from the list. Click Next.
4. On the Schedule screen, leave Always Process Data selected. Click Next.
5. On the Alert screen, enable Generate Alert and select Security Issue from the Alert Severity list. Click Next.

6. On the Alert Suppression screen, uncheck the Suppress Duplicate Alerts option. With this setting disabled, an alert is generated each time the Windows security event is recorded. Click Next.
7. On the Response screen, click the Add button and select Send a Notification to a Notification Group from the list. Select Security Administrators from the Notification group list. Click OK and then click Next.
8. Feel free to enter knowledge specific to this alert rule by clicking the Edit button. Click Next to continue.
9. In the Rule Name field, type **Account Lockout Alert** and click Finish.

The next rule is slightly more challenging because an alert should be generated whenever a member is added to an administrative group. A unique event is generated when a user is added to a local group, a global group, or a universal group. If we configured the alert to respond to these three events, most environments would generate an unmanageable number of alerts. To reduce the number of alerts we have to add an additional criterion that filters the events that we are not interested in. Most group changes within an environment are acceptable and do not pose any substantial security risk; however, several key administrative groups can be identified. These would include

- Domain Admins
- Enterprise Admins
- Schema Admins

Domain Admins is a global group, and both Enterprise Admins and Schema Admins are universal groups (in a native mode domain). To monitor for these events two rules will be created, one to respond to event 632 and another to respond to event 660. To filter global and universal group change alerts that were generated by nonadministrative groups, an advanced criteria filter can be applied to the various parameters within the event. To design the filter we need to identify what parameter corresponds to the name of the group. The simplest method to determine this would be to simulate the action and then review the Parameters tab of the event.

Can't See Any Parameters?

Remember, the parameters for an event are collected only when collection event rules are used. Additionally, the collection event rules can be configured to store only specific parameters or no parameters at all. If you cannot see the parameters associated with an event, double-check the event configuration.

If the collection rules discussed earlier in this chapter (in the "Creating Collection Rules" section) have already been created and applied to your target system, you can simply generate a test event by adding someone to a global group. Figure 20.14 shows an example of the Parameter tab associated with this security event. You can see that the

name of the group is located in Parameter 3; with this information, the advanced criteria for the alert rule can be configured.

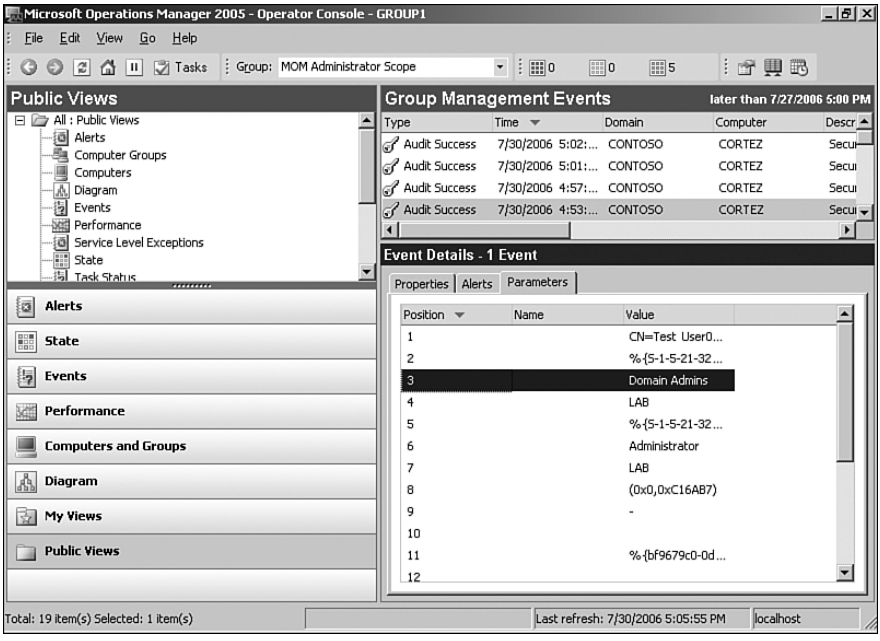


FIGURE 20.14 Event Parameters tab.

Use the following procedure to generate an alert when someone is added to the Domain Admins global group:

1. In the Administrator console, navigate to Management Packs \ Rule Groups \ Security Event Monitoring \ Security Group Management. Right-click Event Rules and select Alert on or Respond to Event.
2. On the Data Provider screen, select Security from the Provider Name list. Click Next.
3. On the Criteria screen, enable With Event ID and enter **632** in the field provided. Enable Of Type and select Success Audit from the list. Click the Advanced button.
4. On the Advanced Criteria screen, select Parameter 3 from the Field list. Select Contains Substring from the Condition list; then type **Domain Admins** in the value field. Click Add to List. Figure 20.15 shows an example of the Advanced Criteria screen. Close the Advanced Criteria screen. Click Next.
5. On the Schedule screen, leave Always Process Data selected. Click Next.
6. On the Alert screen, enable Generate Alert and select Security Issue from the Alert Severity list. Click Next.

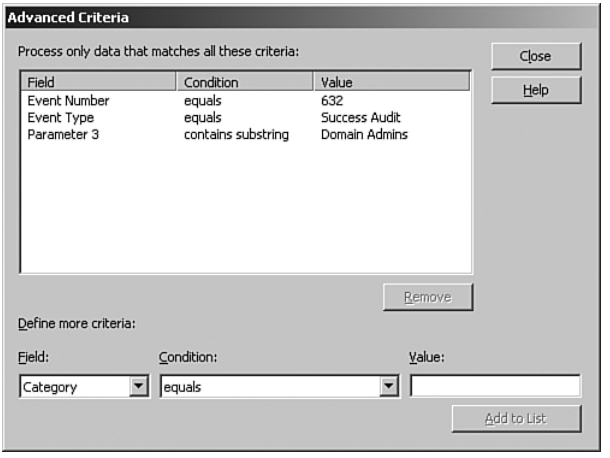


FIGURE 20.15 Advanced Criteria: Contains Substring.

7. On the Alert Suppression screen, uncheck the Suppress Duplicate Alerts option. With this setting disabled, an alert is generated each time the Windows security event is recorded. Click Next.
8. On the Response screen, do not add a response because a single response rule will be added later to respond to all alerts. Click Next.
9. Feel free to enter knowledge specific to this alert rule by clicking the Edit button. Click Next.
10. In the Rule Name field, enter **An account was added to an administrative global security group**. Click Finish.

To detect changes to the Schema Admins and Enterprise Admins groups the alert configuration is slightly different. Follow the same as with the Domain Admins group, but the Event ID for the alert will be 660. Then on the Advanced Criteria screen, select Parameter 3 from the Field list. Select Matches Regular Expression from the Condition list, and finally enter the following regular expression in the value field:

```
(Enterprise.Admins)¦(Schema.Admins)
```

Figure 20.16 shows an example of the Advanced Criteria screen with the correct regular expression configured. The name of this rule can be called "An account was added to an administrative universal security group."

Learning how to write regular expressions is useful. A wealth of training material is available on the Internet along with various web-based testing kits that allow the testing of the regular expression code (such as http://www.fileformat.info/tool/regex.htm and http://www.regexlib.com/CheatSheet.aspx). The regular expression used to identify our universal administrative groups is composed of several elements. The text in the round

brackets "(...)" is the text we want to match in Parameter 3 of the event, and the pipe "|" symbol is an "or" equivalent. Finally, because regular expressions do not allow spaces within the text group, a dot "." was entered. The dot "." represents the space character between the words "Schema" and "Admin" found within the text group.

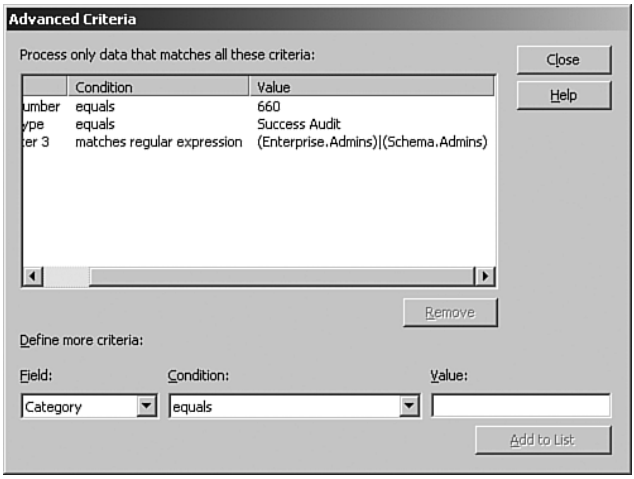


FIGURE 20.16 Advanced Criteria: Regular Expression.

The alert rules we added were not configured to generate a response when an alert is triggered. Because multiple events in the rule group are configured to generate an alert, it is simpler to add a single response rule for all alerts instead of trying to manage each response independently. Follow these steps to set up a response for these rules:

1. In the Administrator console, navigate to Management Packs \ Rule Groups \ Security Event Monitoring \ Security Group Management. Right-click Alert Rules and select Create an Alert Rule.
2. On the Criteria screen, check the Of Severity option and select Security Issue from the list. Check the Only Match Alerts Generated By Rules in the Following Group option, click the Browse button and select the Security Group Management rule group located within the Security Event Monitoring rule group. Click OK; then click Next.
3. On the Schedule screen, leave Always Process Data selected. Click Next.
4. On the Response screen, click the Add button and select Send a Notification to a Notification Group from the list. Select Security Administrators from the Notification Group list. Click OK and then click Next.
5. Feel free to enter knowledge specific to this alert rule by clicking the Edit button. Click Next to continue.
6. In the Rule Name field, type **Account was added to an Administrative Group**. Click Finish.

The final alert is more complicated because an alert is required if more than 15 failed logon events occur within 1 minute. This type of alert is dependant on a consolidation rule. A consolidation rule counts the number of times an event is generated over a specific time period. The count is reset when the time period has elapsed. The alert rule looks at the repeat count of the event and generates an alert only if the count has exceeded the predefined threshold.

Auditing Failed Logon Attempts

For the following rules to work correctly, auditing account logon failures must be enabled. Auditing for domain controllers can be enabled through the Default Domain Controller Security Settings management console.

To create the consolidation rule for our alert perform the following steps:

1. In the Administrator console, navigate to Management Packs \ Rule Groups \ Security Event Monitoring \ Account Logon Activity. Right-click Event Rules and select Consolidate Similar Events.
2. On the Data Provider screen, select Security from the Provider Name list. Click Next.
3. On the Criteria screen, enable With Event ID and enter **675** in the field provided. Enable Of Type and select Failure Audit from the list. Click Next.
4. On the Schedule screen, leave Always Process Data selected. Click Next.
5. On the Consolidate screen, leave the Event Number and Source Name fields checked. Change the Events Must Occur Within value to 60 seconds. Click Next.
6. Enter any knowledge specific to this alert rule by selecting the Edit button. Click Next to continue.
7. In the Rule Name field, type **Count of incorrect password logon events over 1 minute**. Click Finish.
8. Repeat this process to add a consolidation rule for the logon event Authentication ticket request failed (disabled account).

After the consolidation rules have been added, you can create a rule that responds when the repeat count exceeds 15 over the 1 minute (60 second) window. To create the alert rule, do the following:

1. In the Administrator console, navigate to Management Packs \ Rule Groups \ Security Event Monitoring \ Account Logon Activity. Right-click Event Rules and select Alert on or Respond to Event.
2. On the Data Provider screen, select Security in the Provider Name list. Click Next.
3. On the Criteria screen, enable With Event ID and enter **675** in the field provided. Enable Of Type and select Failure Audit from the list. Click the Advanced button.

4. On the Advanced Criteria screen, select Repeat Count from the Field list. Select "is at least" from the Condition list; then type **15** in the Value field. Click Add to List. Figure 20.17 shows an example of the Advanced Criteria screen. Close the Advanced Criteria screen. Click Next.

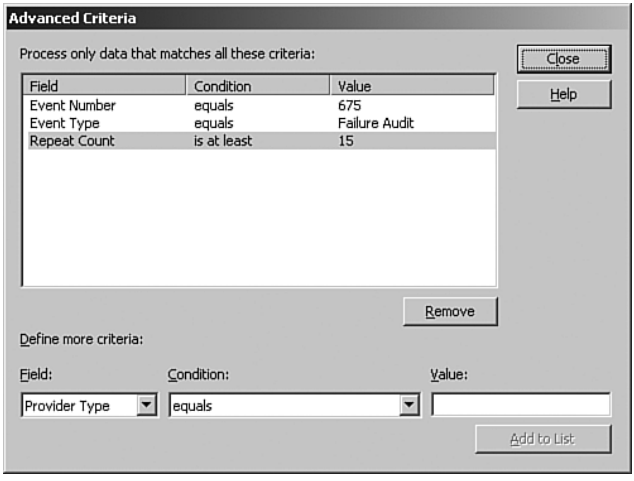


FIGURE 20.17 Repeat Count Advanced Criteria.

5. On the Schedule screen, leave Always Process Data selected. Click Next.
6. On the Alert screen, enable Generate Alert and select Security Issue from the Alert Severity list. Click Next.
7. On the Alert Suppression screen, uncheck the Suppress Duplicate Alerts option. With this setting disabled, an alert is generated each time the Windows security event is recorded. Click Next.
8. On the Response screen, do not add a response because a single response rule will be added later to respond to all alerts. click Next.
9. Specify product knowledge for this alert rule by selecting the Edit button. Click Next.
10. In the Rule Name field, enter **More than 15 incorrect password logon events in 1 minute**. Click Finish.
11. Repeat this process to add a consolidation rule for the logon event Authentication ticket request failed (disabled account).

Creating Operator Tasks

You may have noticed that when security events are captured, the names of various Active Directory objects are recorded by the Globally Unique Identifier (GUID) or Security Identifier (SID), and not the actual name of the object. This makes it difficult to identify

the meaning of some events. To address this problem a registry key must be added to each of the monitored MOM agents. A script (Configure Agents for Security Monitoring.vbs) has been created to help address this problem and is included on the CD accompanying this book.

This script allows an operator to add the correct registry key to a remote system. If the registry key already exists, the script ends, but if the registry key is not found, the script adds the correct key and notifies the operator to restart the MOM agent service. Before setting up this task, the script needs to be added to the script repository through the MOM Administrator console. To add the script to the repository, do the following:

1. In the Administrator console, navigate to Management Packs \ Scripts. Right-click Scripts and select create script.
2. On the General screen, enter **Configure Agents for Security Event Monitoring** in the Name field and enter Adds **the ResolveGUID registry key to the MOM agent** in the Description field. Leave VBScript selected as the language. Click Next.
3. On the Script screen, copy and paste the code found in the Configure Agents for Security Monitoring.vbs file into the script code window. Click Next.
4. On the Parameters screen, click Add for the parameter found in Table 20.4. Click Finish.

TABLE 20.4 Script Parameters

Name	Description	Value
EnableDebug	When the value is set to True, success alerts are generated.	True/False

After the script is added, you can define an operator task. Use the following steps to define a task to execute this script against MOM agents:

1. In the Administrator console, navigate to Management Packs \ Tasks. Right-click Tasks and select Create Task.
2. On the Welcome screen, Click Next.
3. On the Task Run Location and Type screen, select Agent Managed Computer as the location and Script as the type. Click Next.
4. On the Task Configuration screen, select Computer from the Target Role list; then select Configure Agents for Security Event Monitoring from the Script list. Click Next.
5. On the Task Name and Description, enter **Configure Security Translation** in the Name field and **Adds the ResolveGUID registry key to the MOM agent** in the Description field.

You can now manually execute the script against each MOM agent to configure GUID translation and automatically restart the service on the agent.

Creating Operator Views

When developing a management pack it is a good idea to group your data so that whoever is using the Operator console has a clear picture as to what is being monitored. We can create several different views for this management pack.

The following procedure can be used to create a custom view in the Operator console. This view will be configured to display the account lockout alerts. Follow these steps:

1. In the Operator console, select Go \ Public Views.
2. Right-click All: Public Views and select New \ Folder.
3. Name the new folder Security Event Monitoring.
4. Right-click the Security Event Monitoring folder; select New \ Alerts View.
5. On the Alerts View screen, select Alerts that satisfy specified criteria. Click Next.
6. Check With Specified Name from the View list; then click the blue specified link in the Description field.
7. On the Alert Name pop-up window, enter **Account Lockout Alert**. Click OK.
8. Check With Specified Resolution State from the View list; then click the blue specified link in the Description field.
9. On the Resolution State pop-up window, select Display Only Alerts with Resolution State; then select Not Equals "Resolved" from the remaining two drop-down menus. Click OK; then click Next.
10. Enter **Account Lockout** in the View Name field and **All unresolved Account Lockout alerts** in the Description field.

You can repeat this process for the other alerts and events generated by the management pack. For example you can create a view that shows the administrative group change alerts, group management alerts, account management events, and so on. These views are included in the SecurityPack.akm management pack found on the CD accompanying this book.

Installing SecurityPack.akm

If you are interested in using the Security management pack independent of its educational value, you can simply install the management pack rather than manually re-creating it. To install the SecurityPack akm, import it as you would with a normal management pack.

On the CD

The SecurityPack management pack is on the CD included with this book.

The akm file includes the elements that have been discussed throughout this section, such as the computer group, the rule groups, rules, scripts, operator views, and operator tasks.

PingPack Management Pack

One of the most common requests we hear when working on MOM deployments is for a simple management pack that provides notifications of when non-Microsoft systems are not available. This management pack would be used to determine whether an Internet Protocol (IP)-based device is online and responding to a ping. Devices can include a router or firewall, a website, or a non-Windows-based server. Although excellent third-party solutions monitor networking and non-Microsoft servers, some of which we discussed in Chapter 19, addressing this scenario forms the basis of this example of how to create your own management pack.

This sample management pack, which we call *PingPack*, provides a simple ping notification test for IP-addressable devices and is a no-cost ping test solution. The PingPack functionality is not supported by Microsoft or the authors of this book; it is presented merely to give an example of the process to create management packs.

The PingPack is presented here to show a second example of how management packs can be created without using the Management Pack Wizard. At a high level, the process we will use to develop a management pack is to create a rule group, create a computer group, associate the rule group with the computer group, and create the rules for the group. We will also create a task to assist in managing the PingPack.

Creating a Rule Group

This management pack has a specific functionality, and as a result, the rule group structure can be kept simple. We will create a single rule group that will contain the timed event rules needed to execute the PingPack and PingPackServiceDiscovery scripts. This group will also host the different event rules used to control the State view within the Operator console and to alert operators when a network device stops responding to the ping.

The first part of this process is creating a rule group. To create the rule group, perform the following steps:

1. In the Navigation pane of the MOM 2005 Administrator console, go to Management Packs \ Rule Groups. Right-click on Rule Groups and choose Create Rule Group.
2. On the Rule Group Properties page enter **PingPack** for the Name field and enter a description, such as **Management Pack to Ping Server Names**.
3. At the Knowledge Base screen click Edit and enter information to describe the function of the PingPack. Figure 20.18 shows a sample of this content.

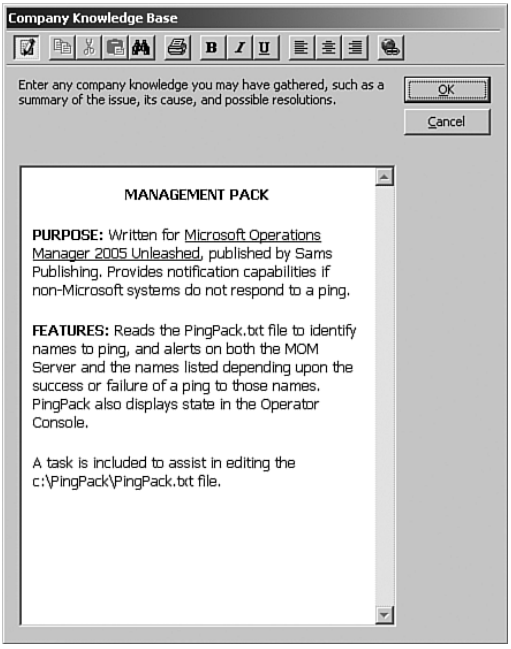


FIGURE 20.18 Rule Group properties—Knowledge Base.

Creating a Computer Group

After creating our rule group, we need to create a computer group that we will then associate with our rule group. This rule group contains one or more servers responsible for executing the PingPack script; essentially the "ping" action is initiated from the computer in this group. In the "SecurityPack Management Pack" section earlier in this chapter, we discussed how using dynamic groups was preferred due to the objectives of that monitoring scenario. With this management pack, much more control over the group membership is desirable, so creating a computer group with a static list of members is recommended.

To create the computer group, perform the following procedure:

1. In the Administrator console, navigate to Management Packs \ Computer Groups. Right-click on Computer Groups and select Create Computer Group.
2. On the Create Computer Group Wizard – General screen, enter a name and description for the computer group. For the PingPack we are entering a name of **PingPack Server** and a description of **Server to execute pings to the names specified in c:\PingPack\PingPack.txt**.
3. On the Create Computer Group Wizard – Included Subgroups screen take the defaults. Click Next to continue.

4. At the Add Computer screen, add the computer that will execute the PingPack script. The designated computer needs to have the MOM agent installed—in our example we designate the Monarch server as shown in Figure 20.19.

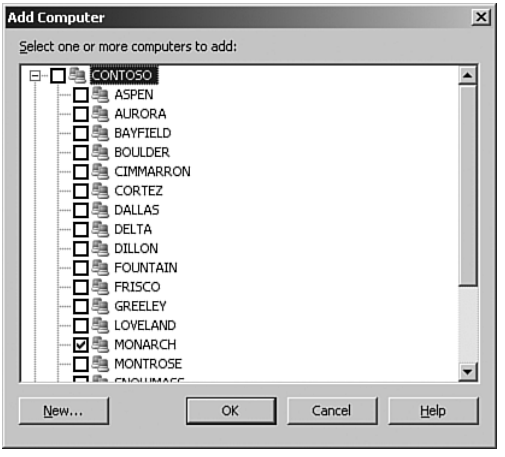


FIGURE 20.19 Add computer to computer group.

5. Take the defaults at the Create Computer Group Wizard – Excluded Computers screen and Create Computer Group Wizard – Search for Computers screens.

6. At the Create Computer Group Wizard – State Roll-up Policy screen take the default value of The Worst State of Any Member Computer or Subgroup, as shown in Figure 20.20. This option indicates that the state of the entire computer group is equal to the most severe state of any member of the computer group. In our example, the only server in the computer group is Monarch, so this setting only matters if more computers are added to the computer group (if Monarch is red due to an error, it will be red regardless of this setting).

7. The Confirm Choices screen, shown in Figure 20.21, summarizes your specifications for the wizard.

The system added to the PingPack Server computer group must be able to "proxy" data for other computers. The PingPack server will essentially ping a list of devices and then send the results of the ping to the management server. The management server knows the results of the ping are for "other" systems. For example, if the PingPack script pings a device called "server1", the PingPack server sends data to the management server for server1; the "server1" object is dynamically created and viewable in the various Operator console views and in the Administrator console under the Unmanaged Computers administrative node.

Agent proxy is beneficial when managing devices that do not have a MOM agent; in this particular example the Operator console treats the "server1" object as almost exactly the same as with a managed agent. The unmanaged system can have performance data, events, and even a dynamic State view as demonstrated with this management pack.

This "proxy" functionality contains inherent dangers. For example, unnecessary data can be inserted into the MOM database, and legitimate managed computers could also have their data modified. By default, the agent-proxy feature is disabled globally. In this type of monitoring scenario, it is common to override the default settings on a single system that is considered trusted.

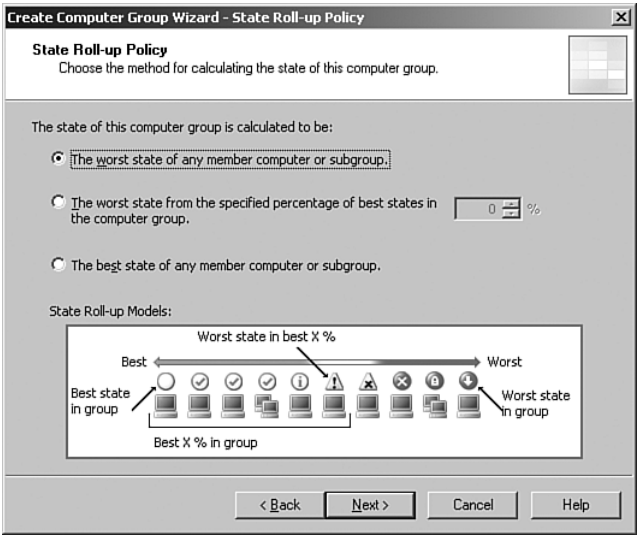


FIGURE 20.20 State Roll-up policy.

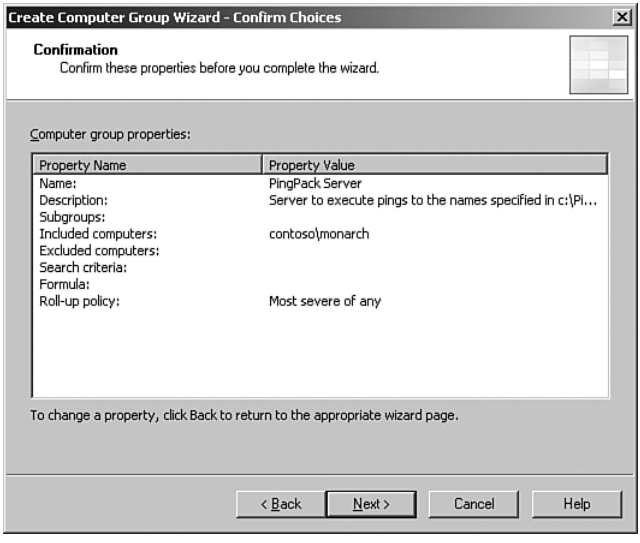


FIGURE 20.21 Create Computer Group Wizard Confirmation screen.

To override the proxy setting and allow the PingPack server to relay data for non-Windows and network devices, do the following:

1. In the Administrator console, go to Administration \ Computers \ Agent-managed Computers. Right-click on the computer you added to the PingPack Server computer group and select Properties.
2. Select the Security tab and uncheck the Use Global Settings option. This will allow the agent proxy settings to be modified.
3. Uncheck the Prevent Agent from Proxy for Other Computers or Network Devices option. Click OK to complete the configuration.

Associating a Computer Group to a Rule Group

After creating the rule group and computer group, you will want to associate the computer group to the rule group. Associating a computer group to a rule group causes the rules to apply to the members of the computer group.

In this example, we are linking the PingPack rules to the Monarch server, which is a member of the PingPack Server computer group. Navigate to Management Packs \ Computer Groups \ PingPack, right-click, and go to the Properties page. On the Computer Groups tab, add the PingPack Server group created in the previous procedure, as shown in Figure 20.22.

FIGURE 20.22 Associate a computer group to the rule group.

Add Rules to Your Rule Group

We now have associated a rule group and a computer group with each other, although we don't have any rules in our management pack. We will build three rules for the PingPack.

The various actions defined in management pack rules, such as collecting events, collecting performance counter data, reading WMI values, executing scripts, and so on, can be performed because of objects called *providers*. The event rules that will execute the PingPack script will use a timed event provider; this type of provider is a schedule that tells the script how to run the script. If you have already imported some of Microsoft's management packs, timed event providers will likely be included to execute the various scripts associated with those management packs. You can use the providers that came with the various management packs that have been imported, or you can create your own.

The following process can be used to create a timed event provider that will be used to execute the PingPack script:

1. In the Administrator console, navigate to Management Packs \ Providers. Right-click on Providers and choose Create Provider.
2. On the Data Provider Type screen, select Timed Event. Click Next.
3. On the Schedule screen, configure the Generate Event Every field for 5 minutes. Enable the Synchronize At option and enter **0:15** in the field provided. Click Finish.

Rule to Run a Script

We first create a scheduled rule that runs a script as a response. This script checks the contents of c:\PingPack\PingPack.txt and executes a ping to each device specified in that file. The PingPack script uses both the Event application log and the internal MOM events to track success or failure of the ping tests. Both types of logging are shown so that the script can be configured to use one or the other as best suits your environment. Using the Event application log provides notification on the server running the script when one of the names fails to ping, while internal MOM events provide status within the PingPack role in the Operator console for each name being pinged.

Finding MOM Events

MOM events appear in the Operator console and are often viewed to determine the results of tasks or other MOM-related events. These events are most quickly located by opening up the Public Views node \ Microsoft Operations Manager \ Operations Manager 2005 \ Scripts and Response Events \ Script Errors Alerts – General section of the Operator console.

If a ping fails the status of the server you specified in the PingPack Server computer group changes to a status of Error. The status of the device that was unable to be pinged also goes to Error on the MOM Operator console.

To create the rule that will run the PingPack script, do the following:

1. In the Administrator console, navigate to Management Packs \ Computer Groups \ PingPack \ Event Rules. Right-click on Event Rules and choose Create Event Rule.
2. On the Select Event Rule Type screen, choose the Alert on or Respond to Event (Event) option from the listing.
3. At the Event Rule Properties – Data Provider screen select the drop-down at the Provider Name field and choose the Schedule Every 5 Minutes Synchronize at 00:15 option from the drop-down list. This option specifies the time of day to begin generating the timed events. For this case we synchronize at 00:15 and run every 5 minutes. Additional information on how synchronization works is available from Microsoft at http://support.microsoft.com/kb/297806/.
4. For the Schedule and Alert Suppression screens take the defaults and continue.
5. At the Responses screen select Add; then choose Launch a Script from the drop-down to bring up the Launch a Script screen. Take the default run location and click the New button.
6. Create a new script. You can name this the PingPack Script. Use the information displayed in Figure 20.23 to fill in the Script Properties on the General tab. Be sure to specify the language as VBScript.

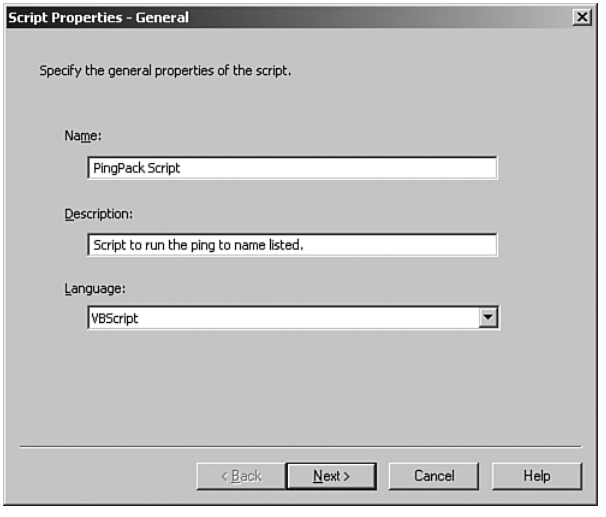


FIGURE 20.23 Script properties.

7. Add the PingPack VBScript code from the CD included with this book into the Script Properties on the Script tab. This code pings the names listed in the c:\PingPack\PingPack.txt file that we create later in this section. Each name listed in the file is pinged, and its success or failure is logged to the Application event log and to the MOM events available within the Operator console.

8. At the Event Rule Properties – Knowledge Base screen, click Edit and add Company Knowledgebase information, which for our example is **Event to call the pingpack vb script**.
9. On the Event Rule Properties – General screen, enter a rule name of **Script – PingPack Execution**. Take the default that This Rule Is Enabled and click Finish to complete creating this rule.

We now have a rule to run the PingPack script.

On the CD

The PingPack and PingPack Discovery scripts can be found on the CD included with this book.

The PingPack Script

The following code shows the code contained within the PingPack script. With this script along with the different event rules, the various functionality provided with the PingPack Management Pack can be achieved.

```
'************ CONSTANTS ************

' Script Specific Constants
Const MAX_REPEAT_COUNT = 2

Const EVENT_TYPE_ERROR = 1
Const EVENT_TYPE_INFORMATION = 4
Const EVENTLOG_TYPE_ERROR = "error"
Const EVENTLOG_TYPE_INFORMATION = "information"

Const INF_PING = "1000"


'************ GLOBAL VARIABLES ************

Dim iErr, strErr

'************ LOADSERVERSFROMFILE ************

Function LoadServersFromFile()

  Dim oFSO, oFile, astrDCs
  Set oFSO = CreateObject("Scripting.FileSystemObject")

  On Error Resume Next
```

```
  Set oFile = oFSO.OpenTextFile("c:\PingPack\PingPack.txt", 1)

    Do Until oFile.AtEndOfStream
      On Error Goto 0
      Dim strLine
      strLine = oFile.ReadLine

      If IsArray(astrDCs) Then
        Dim iSize
        ' LBound is always 0, so with one element, UBound is also 0.
        ' Increment it
        ' by one to make space for the new item.
        iSize = UBound(astrDCs) + 1
        Redim Preserve astrDCs(iSize)
        astrDCs(iSize) = strLine
      Else
        ' Create an array with the first item in it.
        astrDCs = Array(strLine)
      End If
    Loop

  LoadServersFromFile  = astrDCs
End Function

'************ PING ************

Sub PingTest(strComputer)

  On Error Resume Next

  Dim  sReadLine , strCmdLine
  Dim  bPingSuccess
  Dim iAttemptCount
  Dim objShell, objTempFile , objTS , objFSO

   iAttemptCount = 0
   Set objShell = CreateObject("WScript.Shell")

    Do
       set objFSO = CreateObject("Scripting.FileSystemObject")
       With objFSO
            strCmdLine = .BuildPath(.GetSpecialFolder(1), "cmd.exe") _
               & " /c " & .BuildPath(.GetSpecialFolder(1), "ping.exe") _
               & " -n 1 " & strComputer & "  >  PingResults.txt "
       End With
```

```
            objShell.Run strCmdLine, 0, True

      set objTempFile = objFSO.GetFile("PingResults.txt")
      set objTS = objTempFile.OpenAsTextStream(1)

      bPingSuccess = 0
      do while objTs.AtEndOfStream <> true
            sReadLine = objTs.ReadLine
            if instr(lcase(sReadLine), "reply from") > 0 then
                  bPingSuccess = 1
                  exit do
            end if
      loop

      objTS.close
      objTempFile.delete

      Set objTS = nothing
      Set objTempFile = nothing
      Set objFSO = nothing

      iAttemptCount = iAttemptCount + 1
      if   bPingSuccess = 0 then
                  WScript.Sleep 500
      End If

    Loop While (  bPingSuccess = 0 and iAttemptCount < MAX_REPEAT_COUNT )
    '100

    Set objShell = Nothing
    If   bPingSuccess = 0 Then
      iErr = Err.number
      strErr = Err.Description
      On Error Goto 0
            LogMessages 1000, EVENT_TYPE_ERROR, "Ping Failed to " &_
               strComputer, "PingPack", strComputer

  else
      LogMessages 999, EVENT_TYPE_INFORMATION, "Ping Successful to " &_
          strComputer, "PingPack", strComputer
  End If

End Sub
```

```
'************ LOG MESSAGES TO MOM/EVENT LOG ************

Sub LogMessages(EvID, EvType, Desc, Source, Computer)
         LogEvent EvID, EvType, Desc, Source, Computer
         EvLog EvID, EvType, Desc, Source
End Sub

'************ MOM CREATE EVENT ************

Sub CreateEvent(iEventID, iEventType, strMessage, strSource, strComputer)

  On Error Resume Next

  Dim oEvent
  Set oEvent = ScriptContext.CreateEvent
  oEvent.EventNumber = iEventID
  oEvent.EventType = iEventType
  oEvent.Message = strMessage
  oEvent.EventSource = strSource
  oEvent.LoggingComputer = strComputer
  oEvent.SourceComputer = strComputer

  ScriptContext.Submit oEvent

   Set oEvent = nothing
End Sub

'************ MOM LOG EVENT ************
Sub LogEvent(EvID, EvType, Desc, Source, Computer)

  On Error Resume Next
  CreateEvent EvID, EvType, Desc, Source, Computer

End Sub


'************ WRITE TO EVENT LOG  ************

Sub EvLog(EvID, EvType, Desc, Source)

       Dim strCmdLine, strType
       Dim objShell, objFSO

          Set objFSO = CreateObject("Scripting.FileSystemObject")
```

```
        if EvType = EVENT_TYPE_ERROR then
               strType = EVENTLOG_TYPE_ERROR
        end if

        if EvType = EVENT_TYPE_INFORMATION then
              strType = EVENTLOG_TYPE_INFORMATION
        end if

        With objFSO
          strCmdLine = .BuildPath(.GetSpecialFolder(1), "eventcreate.exe") _
          & " /t " & strType & " /id " & EvID & " /l application /so " & _
          Source & "  /d " &  chr(34) & Desc & chr(34)
        End With

        Set objShell = CreateObject("WScript.Shell")
        objShell.Run strCmdLine, 1, True

        Set objShell = nothing
        Set objFSO = nothing
End Sub

'************ MAIN ************

Sub Main()
    Dim aServers, iIndex
    Dim strLine

    aServers = LoadServersFromFile()

     For iIndex = 0 To UBound(aServers)
        strLine = aServers(iIndex)
        PingTest(strLine)
     Next

End Sub

'************ END ALL FUNCTIONS ************
```

State View Roles

The State view in the MOM 2005 Operator console has the capability to present multiple roles depending on the management packs installed in your environment. A *role* is the function of a server that you are monitoring. For example, the MOM 2005 management pack includes the MOM Agent and MOM Server roles. The Exchange 2003 management pack adds the Exchange and Exchange FrontEnd server roles.

For our PingPack MP, we will create a PingPack role. This role is created as a result of the PingPack MOM Alerts rule. To make this happen we have specified to Enable State Alert Properties on the Alert tab of the rule. Within the details of this alert it creates a success alert if it finds a 999 event number and an error alert if it finds an event number of 1000. This alert is created for the PingPack role as specified on the Alert tab. The details of this configuration are discussed in steps 6 and 7 of the following "Check Results from the Script" section.

Check Results from the Script

Next we need a rule that checks the event log for results from the script. The rule causes the state of the role for a particular instance of a server running PingPack to change color depending on the results of the ping tests performed on the names specified in the file. To create this rule we open up Management Packs \ Computer Groups \ PingPack \ Event Rules. Once again, right-click on Event Rules and choose Create Event Rule. Then follow these steps:

1. On the Select Event Rule Type screen choose the Alert on or Respond to Event (Event) option from the listing.
2. On the Event Rule Properties – Data Provider screen choose Application from the Provider Name drop-down list.
3. On the Event Rule Properties – Criteria page fill out the screen as shown in Figure 20.24.

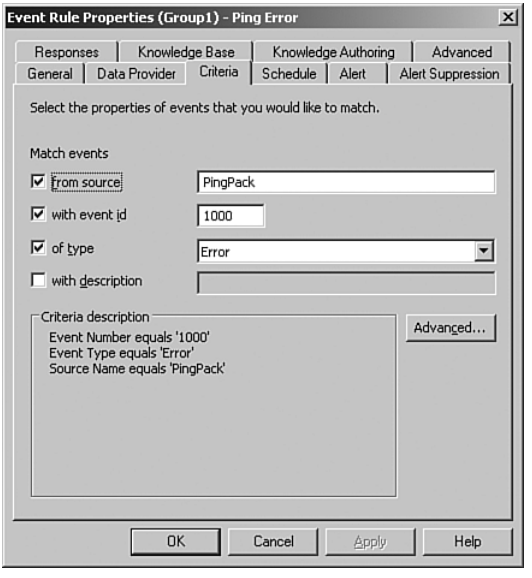


FIGURE 20.24 Event Rule properties criteria.

4. Take the defaults on the Schedule screen.
5. On the Event Rule Properties – Alert page check the Generate Alert check box. Also, check the Enable State Alert Properties check box. Click Edit on the alert properties.
6. On the Alert Severity Calculation for Rule State screen specify the information provided in Figure 20.25. This states that if the event number is 1000, it is an error, and if the event is 999 it is a success.

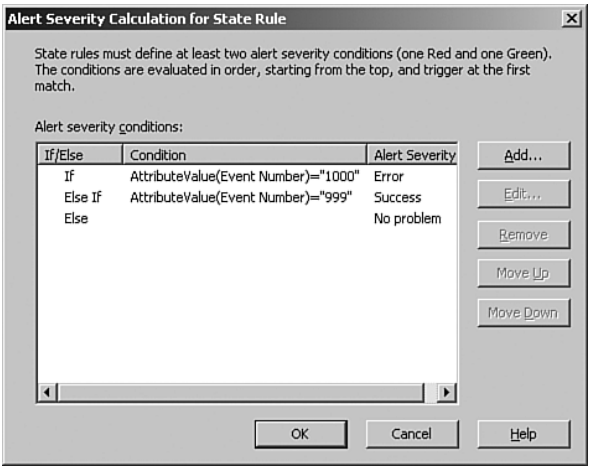


FIGURE 20.25 Alert Severity calculation for state rule.

7. On the Event Rule Properties – Alert page choose PingPack for the server role (which we created in the "State View Roles" section), specify the instance of $Source Computer$, and select the Role component as shown in Figure 20.26.
8. Take the defaults and complete the process. On the General tab, name the rule **PingPack Event Alerts**.

Integrate Non-Windows Devices in the State View

The final rule in our management pack provides alerts to the Operator console within the State view. This rule takes information logged in to MOM events and enables the names included in the PingPack.txt file to be displayed in the State view of the Operator console; the state is dependant on whether the ping was successful or failed. To create this rule, right-click on Event Rules and choose Create Event Rule:

1. Choose the provider name of Script-Generated Data and click Next.
2. On the Event Rule Properties – Criteria screen check the From Source box and type **PingPack** in the field next to it. Click Next to continue.
3. On the Event Rule Properties – Alert page check the Generate Alert check box. Also check the Enable State Alert Properties check box. Click Edit on the alert properties.

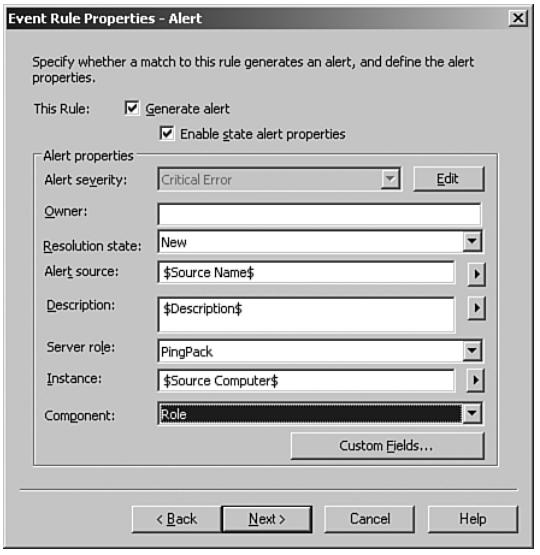


FIGURE 20.26 Event Rule properties – Alert screen.

4. At the Alert Severity Calculation for Rule State screen use the information previously provided in Figure 20.25, which states that if the event number is 1000 it is an error and if it is 999 it is a success.
5. On the Event Rule Properties – Alert page choose values of PingPack for the server role: `$Source Computer$` for the Alert Source and Instance, and Role for the Component.
6. Take the defaults for the rest of the process, and on the Event Rule Properties – General screen enter the rule name of **PingPack MOM Alerts** to complete the rule.

Windows DNS Cache

If the server initiating the ping fails to resolve the name of the target, successive pings from this system will fail even if the device being pinged comes back online. This is caused by the DNS client cache on the PingPack server. The cache remembers the failed resolution attempt and doesn't attempt to resolve the name again until the cache expires or the system is restarted. Disabling the DNS cache on the PingPack server is highly recommended to avoid this issue. The following Microsoft article describes how to disable the DNS cache: http://support.microsoft.com/kb/318803/.

Build a File of Devices That Pingpack Will Ping

The last step in our process is creating a file that contains a list of names or IP addresses to be called by the PingPack. First create a folder at the root of the C: drive named **PingPack**. To create the file, use Notepad on the server that will run the management

pack (this is usually a management server) and name it **c:\PingPack\PingPack.txt**. The file needs to include the names you want the PingPack to use. The names in this file must be resolvable to IP addresses by the server either through DNS resolution or by providing a record in the host file on the server running the PingPack.

Using a Hosts File

If you do not want to use DNS to resolve names of your Non-Windows devices you can use a hosts file on the server where PingPack is running. The host file is located at *%SYSTEMROOT%*\system32\drivers\etc\.

A sample version of the PingPack.txt file content follows:

```
Router1
Router2
Server1
```

Correct PingPack.txt Contents

The correct format for the PingPack.txt file is shown in the previous example, which has one name per line and no blank lines in the file. If the file contains blank lines, or the PingPack.txt is empty or does not exist, errors that show PingPack scripts running over 300 seconds will appear in the Operator console until the issue is resolved. We include this sample file with the CD.

After we create a folder to store the PingPack file and add content to it we need to share the C:\PingPack folder. When sharing the folder give both the account accessing the MOM Operator console and MOM Action account on the server running the PingPack full control access to the folder. Finally, verify that both accounts have full control access to the PingPack folder from a file permission perspective.

Next, we can create a task that will open this file using Notepad from the Operator console. This task simplifies finding the file and managing the list of names or IP addresses to ping. (Remember, this is a highly simplified example to illustrate how to create tasks.) Follow these steps:

1. Within the Administrator console under Management Packs \ Tasks, right-click and choose the option to create a folder for our task. Create the folder with a name of **PingPack**.
2. After creating the folder that will hold our new task, open the folder and right-click to create a task as shown in Figure 20.27.
3. Selecting Create Task starts the Create Task Wizard, which walks us through the process to create the task. On the first screen click Next to continue to the Task Run Location and Type screen. This screen, shown in Figure 20.28, provides choices for where the task will run (Operator console, Management Server, Agent-Managed Computer, Agent-Managed Computer If Available; If Not, on the Management

Server) and the type of task to run. For our task we will run a command line on the Operator console.

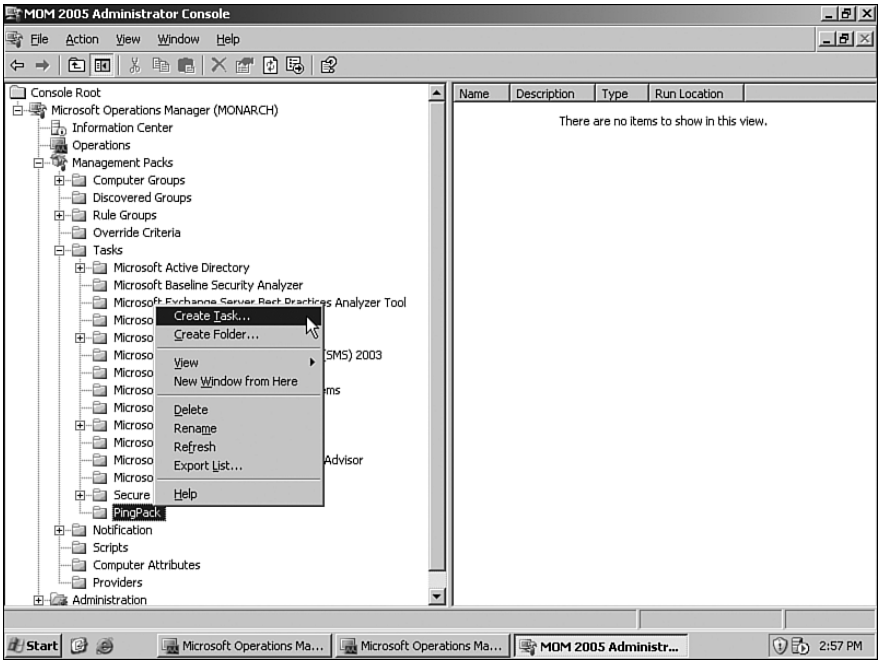


FIGURE 20.27 Create the PingPack task.

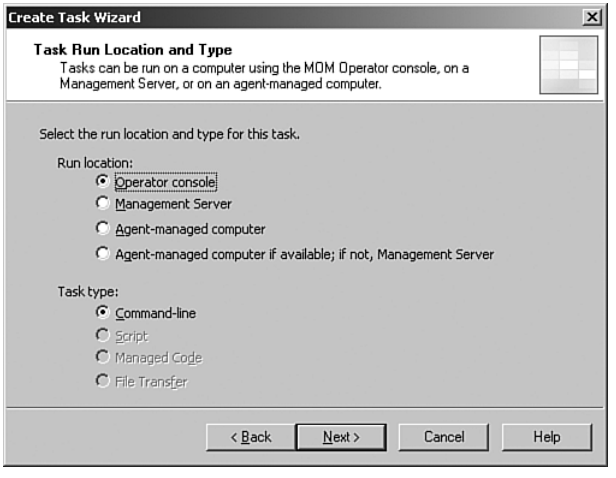


FIGURE 20.28 Configure the task run location and type.

Four different types of tasks can be run: Script, Managed Code, File Transfer, and Command-Line.

- Script tasks provide a method to run MOM scripts (available in the MOM Administrator console under Management Packs \ Scripts). The default parameters for the script can be overridden when creating a task that uses scripts.
- Managed Code tasks can be used to call managed code (that is, code that has its execution managed by the .NET Framework Common Language Runtime).
- File Transfer tasks can be used to upload or download files using BITS (Background Intelligent Transfer Service) using the HTTP protocol. This task supports the uploading of a single file or downloading of multiple files.
- Command-Line tasks run command-line tools or applications. The command line can be configured to use variables such as the $Computer Name$ variable, which we will be using later in the creation of our PingPack task.

4. The next screen is the Task Creation screen where we describe what the task will perform. This includes the View Type, where the task will be visible within the Operator console, and the task command line that specifies where the task will start and the output behavior. For our task the view type will be Computers, the command line is **notepad \\$Computer Name$\PingPack\PingPack.txt**, and the task output behavior is set to not display output. These options are displayed in Figure 20.29.

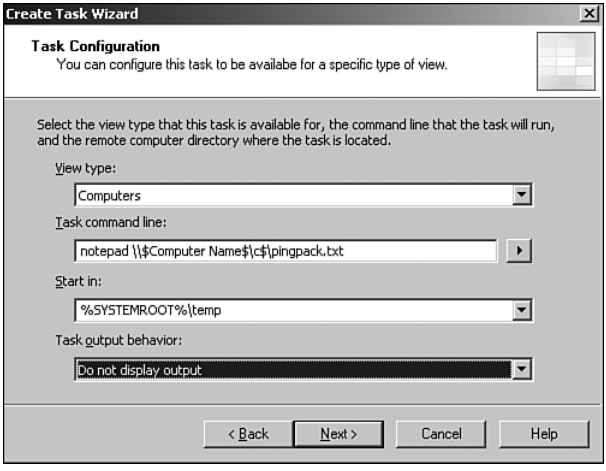


FIGURE 20.29 Configure the details on the task.

5. At the Task Name and Description screen (see Figure 20.30), enter a task name of **Edit PingPack File** and a description of **Edit the file which contains the names to ping**. We could also configure a shortcut key to execute this task—but we will not at this time because the task will be used infrequently. Take the defaults for the remainder of the wizard process to complete creating the task.

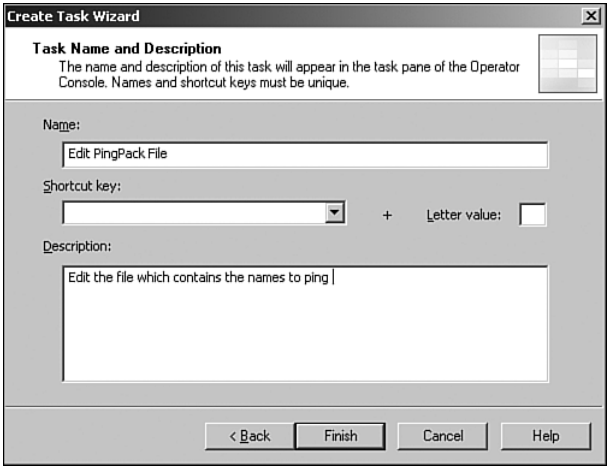


FIGURE 20.30 Configure the name and description for the task.

To execute the task, open the Operator console or press Ctrl+F5 to refresh the console if it is already open. In the Operator console, highlight the server that will run the PingPack scripts (as a reminder this is usually the management server). Open the PingPack task folder and click on the Edit PingPack File option to open the file in Notepad as shown in Figure 20.31. After making changes, save the text file.

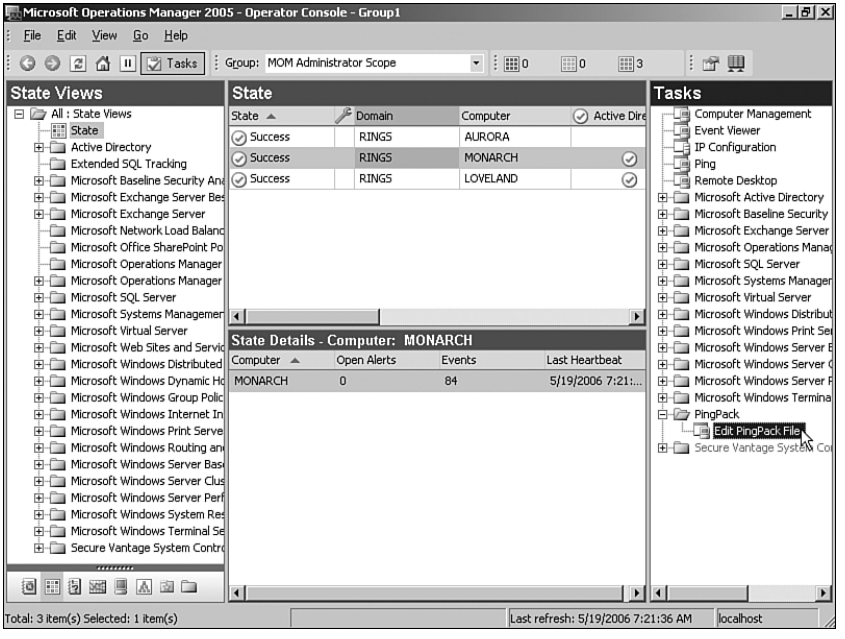


FIGURE 20.31 Launching the Edit PingPack File task.

To activate the management pack, commit the configuration changes. You can then monitor the event log on the server where you activated PingPack or review the Operator console events to determine the status of the names that you want to monitor. Figure 20.32 shows an example of the Operator console that includes multiple non-Windows systems being contacted with the PingPack Management Pack.

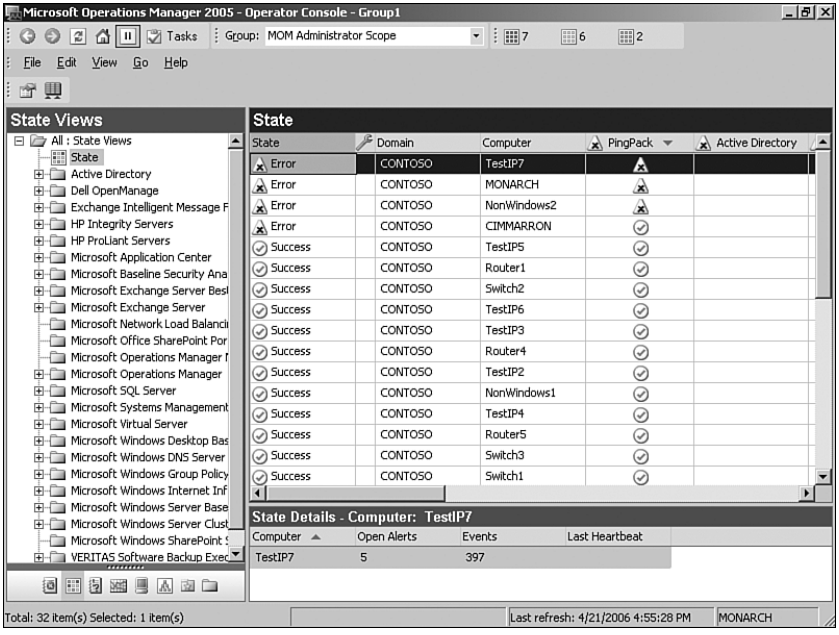


FIGURE 20.32 Operator console with PingPack installed.

Install PingPack.akm

If you are interested in using the PingPack MP independent of its educational value, you can simply install the PingPack MP rather than manually re-creating it. To install the PingPack akm, import it as you would with a normal management pack. No reports are included with PingPack.

On the CD

As was the case with its scripts, the PingPack management pack is on the CD included with this book.

The akm file includes the PingPack computer group, where you will need to specify the name of your management server or the server you designate to run the PingPack scripts. The akm file also creates the PingPack rule group and the task to edit the PingPack text file. The rule group includes the three rules we created previously. You must create the

c:\PingPack\PingPack.txt file—ensuring that name resolution works for each name listed in the file. Be sure to list one system per line in the file.

Next Steps for the PingPack

With some small modifications, the PingPack.vbs can be updated to provide some additional functionality. These changes demonstrate some of the rich scripting features available within the MOM scripting context. If you're interested, a new script with these changes already made is included on the CD accompanying this book. This script is named Monitor Network Systems.vbs.

Adding Parameters

Adding parameters to the script is a great way to provide flexibility over how the script is executed. For example, it is common to add a script parameter to control the events that are generated. If you were monitoring many network devices, an event would be sent to the management server and recorded in the database for each device every time the script ran. Over time this could result in a substantial amount of data. By adding a "debug" parameter you can easily turn off the "successful" events when they aren't needed, allowing the monitoring environment to operator more efficiently.

Another parameter can be added that lists the devices that need to be pinged. This provides centralized management of each device list. Each rule that executes the script can have an independent list of devices, and all rules are managed centrally through the MOM Administrator console.

Implementing the WMI Ping

The PingPack script implements the shell object to run the ping.exe command. This functionality can be changed to use the WMI ping functionality. With a WMI ping, the script can interact with the various properties directly. This offers a greater level of control over the script's execution. However, it is important to note the WMI ping server must be either Windows XP or Windows 2003 or later because this WMI ping functionality does not exist in Windows 2000.

Collecting Ping Performance

When using the WMI ping functionality, the response time of the ping can be easily collected and submitted as performance data. This provides the ability to build a report showing various response trends throughout the environment.

Using State Variables

A state variable can be implemented to store the last result of the ping; this allows the script to track information such as the previous status of the device. By knowing the previous state of the device an alert can be generated when a system comes back online.

The Resulting Script

After making the changes and cleaning up the code, the resulting script looks like this:

```
'Build:1.3.12
'*************************************************************
' Monitor Network Systems
'
' Purpose: Initiates a WMI ping to a network system, script must
'          be executed from a system with a MOM agent installed.
'
' Parameters:
'   EnableDebug - (True/False) When enabled success events
'                  are generated
'
'   CollectPerformance - (True/False) When enabled the ping
'                         response time is sent to the management
'                         server as performance data.
'
'   CollectAvailability - (True/False) When enabled system
'                          availability state data is
'                          generated
'
'   DeviceList - (SERVER1,SERVER2) A comma separated list of
'                 network devices or servers to be monitored
'*************************************************************

'mom constants
const EVENT_TYPE_SUCCESS = 0
const EVENT_TYPE_ERROR = 1
const EVENT_TYPE_WARNING = 2
const EVENT_TYPE_INFORMATION = 4
const EVENT_TYPE_AUDITSUCCESS = 8
const EVENT_TYPE_AUDITFAILURE = 16

'ping constants
const PING_SUCCESS_ID = 999
const PING_FAIL_ID = 1000

const DEVICE_STATUS_ONLINE = "online"
const DEVICE_STATUS_OFFLINE = "offline"

const PING_SUCCESS_MSG = "Ping Successful to "
const PING_FAIL_MSG = "Ping Failed to "

const PING_PERF_OBJECT = "Network System"
const PING_PERF_INSTANCE = "Ping"
```

```
const PING_PERF_COUNTER = "Response Time"

const PING_AVAL_OBJECT = "Network System"
const PING_AVAL_INSTANCE = "Ping"
const PING_AVAL_COUNTER = "Availability"
const PING_AVAL_ONLINE = 1
const PING_AVAL_OFFLINE = 0

'set defaults
dim s_enableDebug, s_enablePerformance, s_deviceList
s_enableDebug = CBool(GetParameter("EnableDebug"))
s_enablePerformance = CBool(GetParameter("CollectPerformance"))
s_enableAvailability = CBool(GetParameter("CollectAvailability"))
s_deviceList = (GetParameter("SystemList"))

' script entry point
sub Main()
  dim a_deviceArray, v_pingResult, s_uniqueDevice

' add each device in the DeviceList parameter to an array
  a_deviceArray = split(s_deviceList, ",")

' ping each device in the array
  for each s_uniqueDevice in a_deviceArray
    v_pingResult = PingDevice(s_uniqueDevice)

'   set the last status varset object to online or offline
    if (v_pingResult = true) then
      call SetLastState(s_uniqueDevice, DEVICE_STATUS_ONLINE)
    else
      call SetLastState(s_uniqueDevice, DEVICE_STATUS_OFFLINE)
    end if
  next
end Sub

'*************************************************************
' PingDevice Function
'
' Purpose: Executes a WMI ping against a network device
'
' Arguments:
'   s_device - The current name of the device being tested
'
' Returns: True, if the ping test is successful
'          False, if the ping test failed
'*************************************************************
```

```
function PingDevice(s_device)

' get the last state of the device
  v_deviceStatus = GetLastState(s_device)

  dim o_pingResults, o_uniquePing, v_deviceStatus
  set o_pingResults = GetObject("winmgmts:" &_
    "{impersonationLevel=impersonate}//./root/cimv2")_
      .ExecQuery("SELECT * FROM Win32_PingStatus " &_
        "WHERE Address = '" & s_device & "'")

  for each o_uniquePing in o_pingResults

'   the status code will be 0 if the ping was successful
    if (o_uniquePing.StatusCode = 0)then
      PingDevice = true

'     if debugging is enabled, or device was offline
'     submit the success event
      if (s_enableDebug = true or _
        v_deviceStatus = DEVICE_STATUS_OFFLINE) then
        call GenerateEvent(s_device, v_deviceStatus,_
          EVENT_TYPE_SUCCESS, PING_SUCCESS_ID,_
            PING_SUCCESS_MSG & ": " & s_device)
      end if

'     submit the ping response time, if parameter is enabled
      if (s_enablePerformance = true) then
        call GeneratePerformance(s_device, PING_PERF_OBJECT,_
          PING_PERF_INSTANCE, PING_PERF_COUNTER,_
            o_uniquePing.ResponseTime)
      end if

'     submit availability data, if parameter is enabled
      if (s_enableAvailability = true) then
        call GeneratePerformance(s_device, PING_AVAL_OBJECT,_
          PING_AVAL_INSTANCE, PING_AVAL_COUNTER,_
            PING_AVAL_ONLINE)
      end if

    else
      PingDevice = false

'     generate an event if the ping fails
      call GenerateEvent(s_device, v_deviceStatus, _
```

```
        EVENT_TYPE_ERROR, PING_FAIL_ID, _
          PING_FAIL_MSG & ": " & s_device & " [" &_
            o_uniquePing.StatusCode & "]")

'     submit the ping response time, if parameter is enabled
      if (s_enablePerformance = true) then
        call GeneratePerformance(s_device, PING_PERF_OBJECT,_
          PING_PERF_INSTANCE, PING_PERF_COUNTER,_
            PING_AVAL_OFFLINE)
      end if

'     submit availability data, if parameter is enabled
      if (s_enableAvailability = true) then
        call GeneratePerformance(s_device, PING_AVAL_OBJECT,_
          PING_AVAL_INSTANCE, PING_AVAL_COUNTER,_
            PING_AVAL_OFFLINE)
      end if

    end if
    scriptContext.Echo("Ping Result [" &_
      s_device & "]  Detail [" & o_uniquePing.StatusCode & "]")
  next
end function

'*****************************************************************
' GetLastState Function
'
' Purpose: Retrieves the last state of the device based on the
'          previous ping test
'
' Arguments:
'   s_deviceName - The name of the monitored device
'
' Returns: The previous state of the device
'*****************************************************************
function GetLastState(s_deviceName)
  dim s_varsetDevice, s_varsetName
  s_varsetDevice = s_deviceName
  s_varsetName = "Last Status"
  dim o_varSet, o_varSetStatus
  set o_varSet = ScriptContext.GetScriptState()
  set o_varSetStatus = o_varSet.GetSet(s_varsetDevice)
  GetLastState = o_varSetStatus.get(s_varsetName)
  scriptContext.Echo("Last State [" &_
```

```
    s_deviceName & "]  Detail [" & GetLastState & "]")
end function

'*****************************************************************
' SetLastState Subroutine
'
' Purpose: Sets the current state of the device based on the
'          most recent ping test
'
' Arguments:
'   s_deviceName - The name of the monitored device
'   s_deviceStatus - The current state of the device
'*****************************************************************
sub SetLastState(s_deviceName, s_deviceStatus)
  dim s_varsetDevice, s_varsetName
  s_varsetDevice = s_deviceName
  s_varsetName = "Last Status"
  dim o_varSet, o_varSetStatus
  set o_varSet = ScriptContext.GetScriptState()
  set o_varSetStatus = o_varSet.GetSet(s_varsetDevice)
  call o_varSetStatus.put(s_varsetName, s_deviceStatus)
  call o_varSet.SaveSet(s_varsetDevice, o_varSetStatus)
  scriptContext.Echo("Set State [" &_
    s_deviceName & "]  Detail [" & s_deviceStatus & "]")
end sub

'*****************************************************************
' GenerateEvent Subroutine
'
' Purpose: Causes a script-generated event based on the values
'          passed to the various arguments
'
' Arguments:
'   s_sourceComputer - The source of the generated event
'   s_eventType - The type of the generated event
'   s_eventNumber - The ID of the generated event
'   s_eventMessage - The message of the generated event
'*****************************************************************
sub GenerateEvent(s_sourceComputer, s_computerStatus,_
  s_eventType, s_eventNumber, s_eventMessage)
  on error resume next
  dim o_omEvent
  if (s_enableDebug = false and _
    s_eventType = EVENT_TYPE_SUCCESS and _
      s_computerStatus = DEVICE_STATUS_ONLINE) then
```

```
    exit sub
  else
    set o_omEvent = ScriptContext.CreateEvent
    with o_omEvent
      .SourceComputer = s_sourceComputer
      .LoggingComputer = s_sourceComputer
      .EventType = s_eventType
      .EventNumber = s_eventNumber
      .Message = s_eventMessage
      .SetEventParameter(v_parm1)
    end with
    ScriptContext.Submit o_omEvent
    end if
  scriptContext.Echo("Generate Event [" &_
    s_sourceComputer & "]  Detail [" &_
      s_computerStatus & " ¦ " & s_eventType & " ¦ " &_
        s_eventNumber & " ¦ " & s_eventMessage & "]")
end sub

'*****************************************************************
' GeneratePerformance Subroutine
'
' Purpose: Creates performance data based on the values
'          passed to the various arguments
'
' Arguments:
'   s_sourceComputer - The source of the performance data
'   s_objectName - The name of the performance object
'   s_counterName - The name of the performance counter
'   s_instanceName - The name of the performance instance
'   s_performanceValue - The performance value
'*****************************************************************
sub GeneratePerformance(s_sourceComputer, s_objectName,_
  s_instanceName, s_counterName, s_performanceValue)
  on error resume next
  dim o_omPerfData
  set o_omPerfData = ScriptContext.CreatePerfData
  with o_omPerfData
    .SourceComputer = s_sourceComputer
    .ObjectName = s_objectName
    .CounterName = s_counterName
    .InstanceName = s_instanceName
```

```
    .Value = s_performanceValue
  end with
  scriptContext.Echo("Generate Performance [" &_
    s_sourceComputer & "]  Detail [" &_
      s_objectName & " ¦ " & s_counterName & " ¦ " &_
        s_instanceName & " ¦ " & s_performanceValue & "]")
  ScriptContext.Submit o_omPerfData
end sub

'*************************************************************
' GetParameter Function
'
' Purpose: Retrieves a named parameter value passed to the
'          response script
'
' Arguments:
'   s_parameterName - The name of the parameter
'
' Returns: The value of the parameter
'*************************************************************
function GetParameter(s_parameterName)
  dim s_parameters, s_variable
  set s_parameters = ScriptContext.Parameters
  s_variable = s_Parameters.get(s_parameterName)
  scriptContext.Echo("Found parameter [" & s_variable & "] " &_
    "Type [" & TypeName(s_variable) & "]")
  GetParameter = s_variable
end function
```

Although this is a little more complicated than the original PingPack script, the script is more representative of a production caliber script and would be much more effective to deploy into a production environment.

Network System Monitoring Management Pack

The Monitor System Monitoring management pack is included on the CD accompanying this book. This management pack includes the various event rules to execute the monitoring script, display state information, and generate alerts and performance data. The management pack is linked to a computer group called System Monitoring Ping Server. If you import the management pack remember to add your "ping" host server to this group. Operator console views used to display the data collected have also been included. Tables 20.5 and 20.6 describe the elements found within the management pack.

TABLE 20.5 Event and Performance Rules

Name	Rule Type	Description
Network System Unavailable	Event	Event rule that generates an alert when a monitored network system fails to respond to the ping.
Network System Available	Event	Event rule that generates an alert when a monitored network system returns from being offline. These event rules are also generated when debugging is enabled.
Monitor Network Systems	Timed Event	Event rule that executes the script used to ping network systems. The script parameters within this rule need to be configured with the list of network systems. The timed event provider should also be adjusted for your environment; by default the script is executed every 60 seconds.
Network System Availability State	Performance	Performance threshold rule that controls the Availability state view located within the Network System role.
Network System Performance State	Performance	Performance threshold rule that controls the Performance state view located within the Network System role. The threshold value within this rule should be adjusted for your environment.
Network System Slow Response	Performance	Event rule that generates an alert when a monitored network system is slow to respond to a ping. The threshold value within this rule should be adjusted for your environment.

TABLE 20.6 Operator Views

Name	Type	Description
Network System Availability	Performance	Displays the Network System availability statistics over the last 24 hours. Availability data is only collected if the CollectAvailability script parameter is set to True.
Network System Available	Alert	Displays alerts generated when a system returns from being offline or when debugging is enabled.
Network System Ping Failed	Event	Displays the events generated when a network system is unavailable. These events trigger the Network System Unavailable alerts.

TABLE 20.6 Continued

Name	Type	Description
Network System Ping Response Time	Performance	Displays the Network System ping response times over the last 24 hours. Performance data is only collected if the CollectPerformance script parameter is set to True.
Network System Ping Success	Event	Displays the events generated when a network system is available. This event is only generated when the server comes back online after being offline or if debugging is enabled through the corresponding EnableDebug script parameter.
Network System Slow Response	Alert	Displays alerts generated when the ping response time exceeds the predefined threshold. Performance data is only collected if the CollectPerformance script parameter is set to True.
Network System State	State	The State view looks at the two components within the Network System role. The Performance component displays the state of the ping response time; an "error" state is shown when the response time exceeds the predefined threshold. The Availability component displays the availability status of the system; an "error" is shown when a system is unavailable.
Network System Unavailable	Alert	Displays alerts generated when a network system is unavailable.

Installing the Network System Monitoring Management Pack

To install the Network System Monitoring management pack, perform the following steps:

1. Import the akm file into MOM 2005, using the procedure discussed in Chapter 13.
2. Add the computer to run the Network System Monitoring scripts within the Network System Monitoring Ping Server computer group (referred to as the *ping server*).
3. Verify that the ping server can successfully resolve names and ping by name the network devices that will be monitored.
4. Change the parameters on the Responses tab of the Monitor Network Systems rule to specify the server to monitor (located in Management Packs \ Rule Groups \ Network Systems Monitoring \ Event Rules) within the SystemList parameter. When

adding the names of network devices to be monitored, be sure to not use periods or spaces within the names.

Examples of unacceptable values for the SystemList parameter would include items such as "SERVER1, SERVER2" (because of the space) or "www.contoso.com" (because of the dots). Acceptable values for the SystemList parameter would be items such as "SERVER1,SERVER2" or "Router1,Server1,Router2" (do not type the quotes in any of the values; they are just here to show the content of the parameter).

5. Remember to allow the ping server to "proxy" data for other systems, or you will receive a security alert each time the script is executed and the management server will reject the data. For additional information on how to configure agent proxy settings, refer to the "PingPack Management Pack" section earlier in this chapter.

More on Management Pack Development

Other resources for management pack development include the MOM 2005 Management Pack Development Guide (http://go.microsoft.com/fwlink/?linkid=50020), which provides an overall synopsis in developing your own management packs, and Silect Software's MP Studio Professional.

The MP Studio Professional can be used to test, edit, and tune management packs independent of your MOM environment. Information on this product is available at http://www.silect.com/products/studio_professional/products_pro.htm.

Summary

In this chapter we discussed options available for designing and developing custom management packs. We created four sample management packs that provide guidance for common real-world problems along with tips that will assist in your own management pack development venture. We looked at the simplicity of creating a management pack using the Management Pack Wizard. We discussed the SecurityPack, describing some of the different options available when looking into monitoring security events. We stepped through creation of the PingPack, highlighting the flexibility of MOM by extending monitoring functionality through scripts to generate a State view and alerts for non-Windows and network devices. Finally, we extended the functionality of the PingPack and created a more production-caliber management pack for network monitoring using the Network Systems Monitoring management pack. In the next chapter we will investigate using and developing reports within MOM.

CHAPTER 21

Using and Developing Reports

IN THIS CHAPTER

- MOM Reporting Components
- Using MOM Reporting
- Creating Reports
- Administration

Chapter 20, "Developing Management Packs," demonstrated how to increase the capabilities of MOM 2005 by creating custom management packs. This chapter will discuss using the MOM 2005 Reporting components and extending MOM 2005's functionality even further with custom report development.

Reporting functionality is becoming increasingly important. As business requirements evolve, efficiently maintaining its underlying infrastructure is essential to a company's overall success. One of the most reliable ways to foresee and plan for future infrastructure requirements is understanding current and past infrastructure tendencies. This type of business and strategic planning requires an in-depth understanding of an organization's many different environmental aspects.

MOM 2005 Reporting offers an efficient way to produce accurate reports describing current and historical data collected with your MOM 2005 implementation. This long-term environmental analysis of key business components is invaluable to anyone making infrastructure-based decisions. The data can be used for trend and pattern analysis of business systems and extrapolated to determine growth patterns and future business requirements. For example, as the organization changes, load placed on servers, bandwidth utilization, and storage consumption can be concurrently monitored to determine how the entire environment is reacting to these changes. This type of analysis exposes valuable information such as current scalability, along with possible limitations or future bottlenecks.

This chapter focuses on the different aspects in MOM Reporting. We discuss reporting components, configuring the reporting server, creating reports, and report administration.

MOM Reporting Components

MOM 2005 Reporting is an optional component, providing long-term storage and retrieval functionality for the vast amounts of data collected with your MOM 2005 implementation. The MOM 2005 operational database (OnePoint) needs to be kept relatively small due to the high level of activity and frequent access performed by the management servers, which limits the amount of historical data it can retain. In contrast, the MOM reporting database is not subject to these conditions and as a result can efficiently grow quite large without negative impacts on functionality. The recommended maximum size of the operations database is 30 gigabytes (GB), whereas the reporting database has a suggested maximum size of 1 terabyte (TB) but theoretically can grow to the boundaries of your hardware and underlying operating system.

MOM 2005 Workgroup Edition

The MOM 2005 Reporting feature is not available to users running the MOM 2005 Workgroup Edition. You need the full version of MOM 2005 to employ MOM Reporting.

Microsoft uses several different technologies to greatly enhance MOM 2005's reporting functionality. The current version of MOM Reporting is noticeably superior to its predecessor (MOM 2000) by providing significant out-of-the-box reporting functionality enhancements and advanced customization capabilities, with almost limitless expandability. MOM 2005 Reporting uses the SQL Server Reporting Services (SSRS) engine, and Figure 21.1 shows the relationship between the different components used with MOM 2005 Reporting and SSRS.

MOM 2005 Reporting combines each of the following components, creating an extensible reporting infrastructure:

- MOM reporting database—The MOM reporting database, referred to as "Data Sources" in Figure 21.1, is the foundation of MOM Reporting. This database stores a historical copy of the same data that can be found in the MOM operations database.
- MOM Reporting console—The MOM Reporting console is a folder found in the SQL Reporting Services web page and is accessed using the XML Web Service Interface. This interface is used to access almost all reporting server functionality, including viewing reports, developing new reports, and managing the reporting server.
- DTS job—The Data Transformation Services (DTS) job is the process that copies existing data from the operations database to the reporting database. The DTS job is scheduled with the Windows built-in task scheduler.
- SQL Server Reporting Services—Microsoft SQL Server Reporting Services is one of the key underlying components MOM Reporting is based on. SSRS provides all the features and functionality available in the MOM Reporting console. This includes report processing, rendering, and scheduling and delivery of reports.

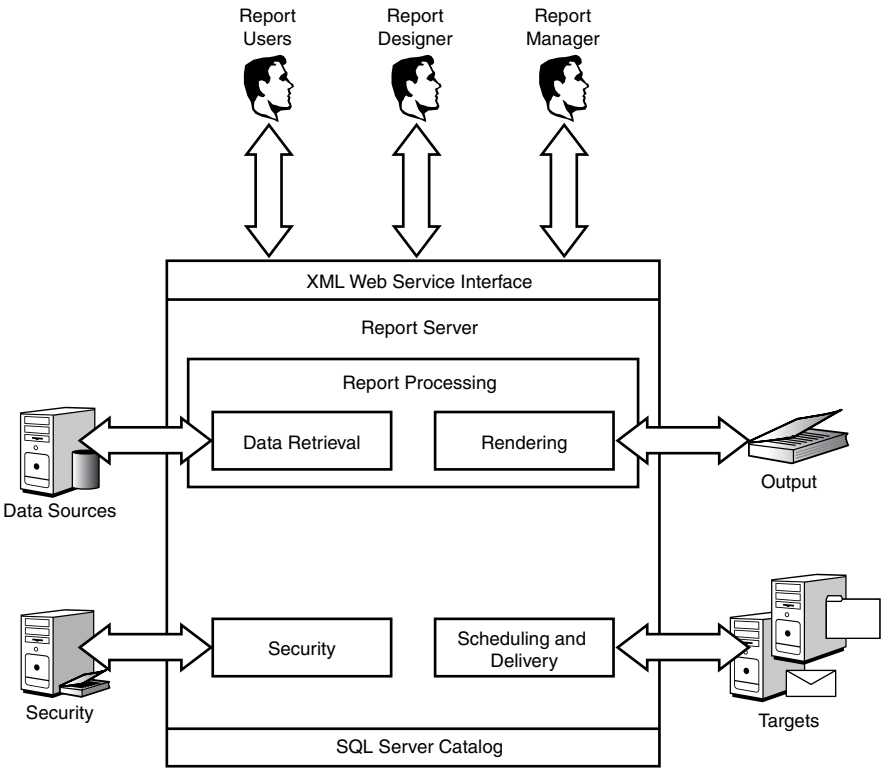


FIGURE 21.1 MOM 2005 Reporting components.

- MOM reports—MOM reports are templates or definitions that contain the business logic used by SSRS to aggregate and render information from the MOM reporting database.
- Report Designer—The report designer is a system using Visual Studio .NET 2003 and the SQL Server Reporting Services client components. The report designer can create new reports or edit existing reports.

Installing MOM Reporting

Review Chapter 6, "Installing MOM 2005," for guidance when installing your MOM reporting infrastructure.

An in-depth knowledge of how MOM Reporting uses each component can translate into a greater overall success for MOM Reporting within your organization. To assist with this understanding, we will review additional details associated with each of the different reporting components.

MOM Reporting Database

The prerequisite verification process required to install MOM Reporting is performed on the server that will host the MOM reporting database. The server hosting this database must be running SQL Server 2000 with at least Service Pack 3a (or SQL Server 2005 if you are using SQL Server 2005 for your MOM 2005 installation). The reporting server installation creates a SQL database named SystemCenterReporting, which is used to store a copy of the data found in the MOM OnePoint database.

We do not recommend hosting the reporting database on the same server hosting the OnePoint database in a medium or large enterprise deployment. Using the same server will most likely lead to performance and scalability problems, potentially negatively impacting business-critical MOM operations. Although it is possible to host both databases on the same server, this may only be acceptable in a smaller environment where the server can easily handle the expected load.

Designing a MOM Reporting Infrastructure

Review Chapter 4, "Planning your MOM Deployment," for infrastructure design and scalability guidance.

The SQL Server database used by MOM Reporting has a comprehensive schema. Microsoft provides documentation describing the SQL views and available data relationships, which can assist in report customization and development. Although we will cover a core subset of these SQL views in the "Creating Reports" section later in this chapter, we recommend becoming familiar with all aspects of the schema if you plan further report customization.

SQL Views Versus Tables

Microsoft does not recommend querying tables directly when retrieving data from the reporting database and suggests that all data should be queried through its predefined SQL views. Although sophisticated SQL architects may not completely agree with this statement, if you're just starting out with SQL coding and report design, we recommend following this suggestion.

Review the MOM reporting schema documentation for detailed information on the many predefined SQL views available for the MOM reporting database. The MOM reporting schema documentation is discussed in Chapter 8 of the Management Pack Deployment Guide, which can be accessed at http://go.microsoft.com/fwlink/?linkid=50020.

MOM Reporting Console

The MOM 2005 Reporting setup program automatically installs the MOM Reporting console on the server running SQL 2000 Reporting Services. The console consists of a folder called Microsoft Operations Manager Reporting, located within the SQL Reporting Services web page. This folder contains the MOM report definitions, images used in the

reports, and the data source used by the report definitions to access the reporting database. All functionality within the MOM Reporting console is provided by the underlying SQL Server Reporting Services. In the "Using MOM Reporting" and "Administration" sections later in the chapter we cover the following functionality related to MOM Reporting:

- Importing and running reports
- Exporting reports
- Creating report subscriptions
- Managing existing subscriptions
- Creating custom folders and linked reports
- Administering site security and roles

MOM Reporting is completely web-based, and almost all possible user and administrative functionality is accessible through the web browser. The Reporting console is the primary method for users and administrators to access data contained within the reporting database.

DTS Job

The DTS job is a process that copies data from the operations database to the reporting database before grooming the data in the operations database. The term *groom* refers to the act of removing old data from the database to make room for new data. By default, grooming is set to 4 days on the operations database and 395 days on the reporting database. The historical data stored in the reporting database provides a longer term view that you can use for trend analysis for servers and applications monitored by MOM. The DTS job is configured automatically during the MOM reporting installation on the server hosting the reporting database. Additional information on how to customize the DTS job can be found in the "Administration" section later in this chapter.

SQL Server Reporting Services (SSRS)

SSRS is a prerequisite component that must be installed and functional before installing the MOM reporting components. During the SSRS installation two SQL Server databases are created that will host the SQL Reporting Services data: ReportServer and ReportServerTempDB.

- The ReportServer database contains all the MOM report definitions, security settings, and scheduling information along with all other configuration data that is not part of the MOM reporting database.
- The ReportServerTempDB database contains temporary data such as user state information and cached reports.

SSRS is the "engine" used by MOM Reporting to aggregate data from the reporting database and render the data, either interactively through the web browser or on a defined schedule. SSRS has the capability to render data in many popular formats, including

- HTML with Office Web Components
- Excel file
- Web archive
- Acrobat PDF file
- TIFF file
- CSV file
- XML with report data

SSRS provides additional features, including the capability to create report subscriptions. A *report subscription* is where a report is delivered through email or copied to a file server based on a predefined schedule. SSRS can also be accessed programmatically with third-party or custom-developed applications.

MOM Reports

The MOM report templates that ship with Microsoft's management packs are XML files. These templates contain specific criteria or business logic defining how data from the reporting database is aggregated. The templates also contain formatting that the data in the report displays while being viewed or rendered in one of the many available formats. Microsoft has developed reports for almost every available Microsoft technology; to date hundreds of reports are available and are bundled in the MOM 2005 management packs. These reports span a wide array of uses, including the following:

- Performance and health analysis
- Configuration analysis
- Alert and event analysis
- Server application specific analysis
- Security and security patch compliance

Report Designer

The report designer is a server or workstation used to develop custom reports. The report designer computer must have Visual Studio .NET 2003 and the SSRS client components installed, with enough system resources to run queries against potentially large amounts of data. Any edition of Visual Studio .NET 2003 can build reports, including the Express edition. A report designer system is used to create new reports or customize existing reports. The SSRS client components are available by running the SSRS setup program and selecting client components from the list of available components.

Using MOM Reporting

All the features in the MOM Reporting console come from the underlying SQL Server Reporting Services. In this section we'll step though several procedures that involve fundamental usages of MOM Reporting. These include:

- Importing reports
- Accessing the MOM Reporting console
- Navigating the site and running reports
- Creating subscriptions and schedules
- Customizing report execution, caching, and snapshots
- Creating linked reports
- Managing folders and reports

Importing Reports

After installing MOM Reporting, you import the report templates to the reporting server. Management packs downloaded from Microsoft's management pack catalog site (http://go.microsoft.com/fwlink/?linkid=43970) are compressed and must be extracted before being imported into the reporting environment. The report templates that come bundled with most Microsoft management packs are typically extracted to the same directory as the management pack .akm files. After extracting the management pack, check for an XML file in the directory where the management pack was extracted. This XML file is the report template you need to upload to the MOM Reporting server.

Typically the report templates are imported to the reporting server when the management packs are imported to the management servers, but this may not always be the case. In certain scenarios the MOM management packs could be deployed before the reporting server installation is complete, so Microsoft provides several methods to import new report templates or update existing report templates on the reporting server.

The simplest method available to import reports is through the built-in Management Pack Import/Export Wizard available in the MOM Administrator console. Figure 21.2 shows the Import/Export menu item within the Administrator console. (You can also access the wizard by right-clicking on Management Packs in the Navigation pane and selecting Import/Export Management Pack.)

For details on how to add reports into MOM using the Management Pack Import/Export Wizard, refer to Chapter 13, "Administering Management Packs." Reports can also be imported or exported with the RptUtil.exe command-line utility. Details on RptUtil are provided in Chapter 12, "Backup and Recovery."

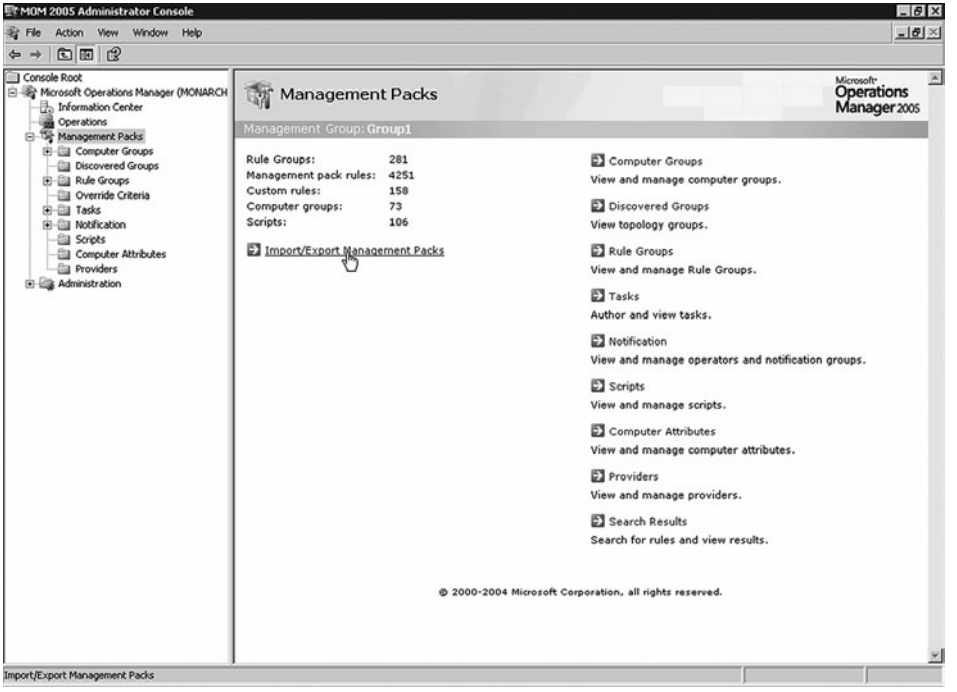


FIGURE 21.2 Launch the Management Pack Import/Export Wizard.

Accessing the MOM Reporting Console

The MOM Reporting console can be opened through both the MOM Administrator console and the MOM Operator console, which allows quick and simple access without needing to know the URL of the MOM reporting server. As an alternative to the methods described in this chapter you can manually launch your browser and type in the URL of the MOM reporting server. This URL is http://<*server name*>/Reports by default.

The following steps demonstrate how to access the MOM Reporting console through the MOM Administrator console. Figure 21.3 shows the Reporting console link.

1. Open the Administrator console.
2. Within the Navigation pane, expand the top-level Microsoft Operations Manager <*management server*> menu item.
3. Select Operations from the Navigation menu and click on the Start Reporting Console link listed in the Details pane.

The following steps demonstrate accessing the MOM Reporting console through the MOM Operations console. Figure 21.4 shows the Reporting console link.

1. Open the Operator Console.
2. Select Go, Open Reporting Console from the menu.

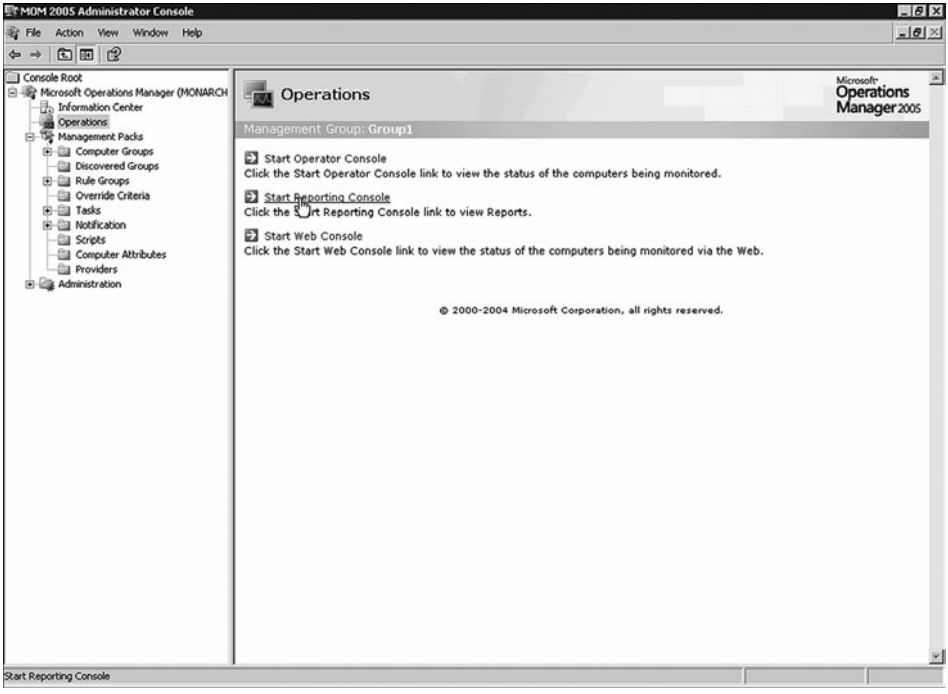


FIGURE 21.3 Accessing the MOM Reporting Console through the Administrator console.

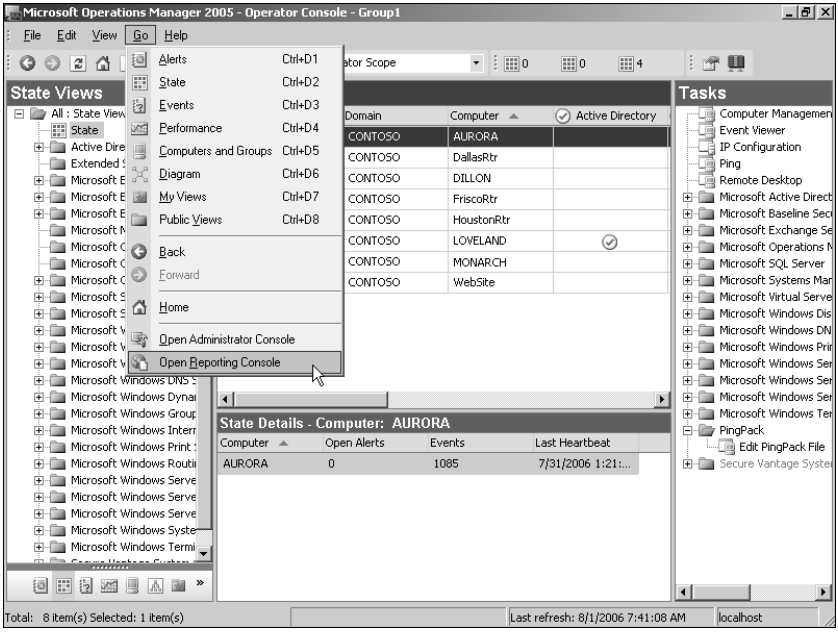


FIGURE 21.4 Accessing the MOM Reporting console through the Operator console.

Navigating the Site and Running Reports

The MOM Reporting console has two primary areas as shown in Figure 21.5. The top section of the page contains common menu and navigational items along with a sitewide menu and a search function. The items in the top area remain relatively consistent as you navigate through the site folder hierarchy and view different reports. The lower area of the reporting console is divided into multiple tabs—Contents and Properties. Each tab displays different information and provides different functionality depending on where you are in the site.

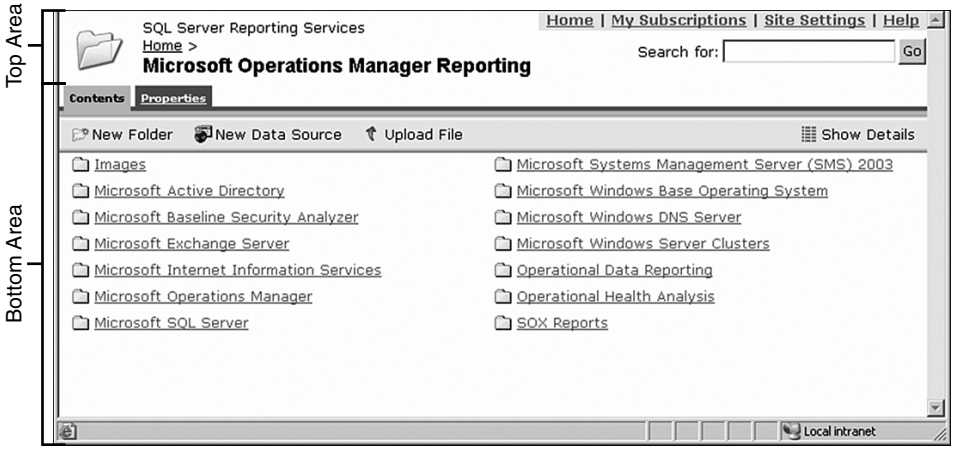


FIGURE 21.5 The MOM Reporting console.

Before proceeding to the next section you should become familiar with some of the navigational features available in the Reporting console. Using these features and menus will help you locate your current position in the site and quickly move from area to area.

Breadcrumbs

As you navigate through the folder hierarchy on the MOM reporting server, a dynamic trail is created near the top left-hand corner of the page. This trail is commonly referred to as a *breadcrumb* navigational trail and offers an easy way to find your way back through the folder hierarchy. By clicking on any of the previous folders listed in the breadcrumb navigational trail you can immediately navigate to that folder. Using the breadcrumb trail is often more efficient than using the Back button on the browser because the Back button often can cause undesired effects when navigating a site with different frames, subareas, and menus.

Figure 21.6 shows the breadcrumb trail created when navigating to the Performance History folder within the Microsoft Windows Base Operating System folder.

Site-Wide Menu

The menu shown in Figure 21.7 is found at the top right-hand corner of the screen. This menu is always available, independent of the area you have navigated to.

FIGURE 21.6 Breadcrumb navigation trail.

FIGURE 21.7 Site-wide menu.

The menu items are as follows:

- Home—Takes you to the root page of the reporting site. From the home page you can select the Microsoft Operations Manager Reporting folder to return to the MOM Reporting console.
- My Subscriptions—Shows a list of report subscriptions you have created. You cannot add new subscriptions from this page, although you can manage existing subscriptions. For example, after the user subscribes to a report, the report is listed in the My Subscriptions area. The user can then edit all aspects of the report subscription including the selected parameters and schedule. The user can also delete the subscription from within this area.
- Site Settings—Available only to users with the appropriate permissions, by default the System Administrator role. The System Administrator role is automatically granted to the local Administrators security group on the report server when the reporting server is deployed. The settings in this area control all of the site-wide settings such as the name of the site and global security options. This area is discussed in the "Administration" section later in this chapter.
- Help—Launches the Report Manager help file in a new window. The help page contains information on the many different aspects of the reporting server, including different user tasks such as running a report and creating a subscription.

Searching the Site

The search tool, shown in Figure 21.8, offers a simple method to search within the Name and Descriptions fields of reports residing on the reporting server. The search tool is aware of security settings associated with reports and folders, so it will not display items the user does not have access to. This search tool does not accept wild-card characters or find data within rendered reports.

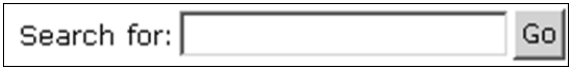


FIGURE 21.8 Search toolbar.

Running Reports

Running reports in the MOM Reporting console is one of the basic methods used to retrieve and display data within the MOM Reporting database. In this example we'll run the Disk Performance Analysis report, located in the Microsoft Windows Base Operating System folder on the reporting server. The Disk Performance report is a chart showing several different disk performance counters for a single computer.

Report Prerequisites

For the Disk Performance report to work you must import the Windows Base Operating System management pack and have successfully executed a DTS job, transferring data into the Reporting database. Refer to the "Administration" section later in this chapter for additional information on the DTS job.

Follow these steps to run the report:

1. Open the MOM Reporting console through the Administrator console or the Operator console.
2. After the console is open, the Contents tab automatically lists the contents of the Microsoft Operations Manager Reporting folder.
3. Click on the Microsoft Windows Base Operating System folder. The Contents tab now displays a list of available reports within the Microsoft Windows Base Operating System folder. Your screen should look similar to the one displayed in Figure 21.9.

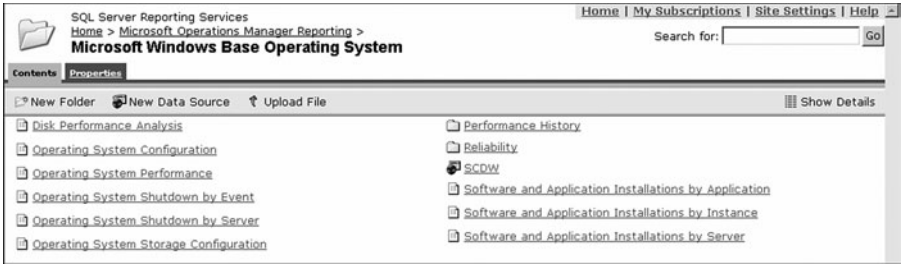


FIGURE 21.9 Microsoft Windows Base Operating System reports.

4. Click on the Disk Performance Analysis report. In a few seconds the report opens and a new set of tabs is displayed. These tabs provide report level functionality, different from the tabs available while navigating the site.
5. Additional parameters are required before the report will show data. The area just below the report tabs has been dynamically created to request the parameters required to run the report. In the Computer Group drop-down list, select Microsoft Windows Servers.

Report Parameters

You may have noticed some of the parameters in the report have been automatically filled in with default values, such as the Begin Date and End Date. Additionally, the Computer Name parameter is grayed out and cannot be selected until the Computer Group parameter is set.

6. After the Microsoft Windows Servers group is selected, the Computer Name parameter is automatically filled in with the name of a managed server that is a member of that computer group. You can leave this default server selected, or select a different server from the drop-down menu.

7. Click the View Report button. A green progress animation is displayed while data for the report is gathered and the report is rendered. In several seconds a graph displays, showing the disk performance analysis for the computer you selected. Your report should look similar to the one shown in Figure 21.10.

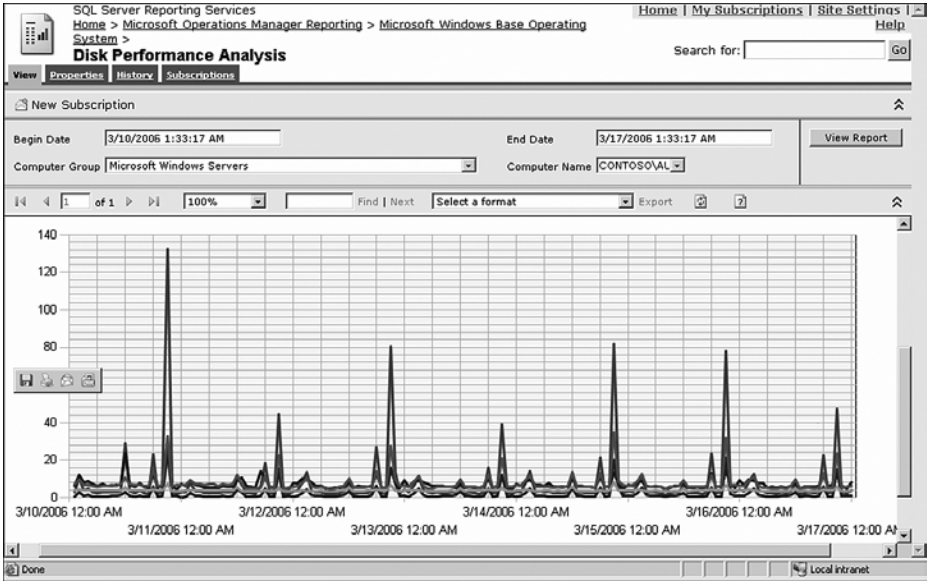


FIGURE 21.10 Disk Performance Analysis graph.

Several options are available while looking at a report. These options are located in the report toolbar located between the report and the report parameters area. From the report toolbar you can navigate through the different pages of the report, zoom in and out of the report, refresh the report content, and export the report to one of the many supported built-in formats such as PDF or Excel.

The report toolbar also shows a search function. This search function is different from the one located in the top area of the Reporting console. The search function located on the report toolbar allows you to search the data contained in the report.

Creating Subscriptions and Schedules

MOM Reporting allows you to schedule reports for delivery based upon subscriptions to the report and to share report schedules.

Subscribing to a Report

MOM Reporting includes the ability to deliver specific reports to intended audiences through an email or file server subscription. This capability allows a targeted audience to view the report without needing to know how to find the reporting server, navigate to the desired report, or understand what parameters they need to run the report.

The following procedure creates a report subscription to deliver to a user or distribution group in your environment:

1. Open the MOM Reporting console, navigate to the Microsoft Operations Manager folder, and click on the Event Logging Latency report.
2. Select the New Subscription button located below the View tab.
3. The first section of the Subscription page lists the Report Delivery Options. In the Delivered By field, leave the Report Server E-Mail option selected.
4. In the To field, enter the email address of the person or distribution list you want the report delivered to. You can enter additional email addresses in the Cc and Bcc fields as necessary.
5. Verify that the Include Report check box has been enabled. Also verify that Web Archive is selected as the Render Format. You can select any of the format types depending on how the reader wants to view the report.
6. The second part of the subscriptions page allows you to configure the delivery schedule. Click the Select Schedule button to open the Schedule Configuration page and set the desired delivery schedule options. Click OK to return to the New Subscription page after the schedule is defined.
7. The final section of the Subscriptions page allows you to configure the report parameters. The Begin Date and End Date are already configured to use the default settings. This report was designed to show a date range of seven days ending on the current date.
8. In the Computer Group field, select Microsoft Windows Servers from the drop-down menu. Alternatively you can select any group of interest in this field.
9. Click the OK button to save the subscription. The Disk Analysis email report subscription is now complete.

When creating a subscription, you can change the delivery method by choosing a different option in the Delivered By drop-down menu. Available delivery options include emailing the report and copying the report to a file server.

Creating Shared Schedules

Part of the subscription creation process includes configuring a schedule. The schedule defines when and how often the report is going to be delivered. You can also create a shared schedule as an alternative to defining a schedule for each subscription. Shared schedules are a great way to standardize report delivery by preconfiguring delivery options.

Shared Schedules

To create a shared schedule you must have the appropriate permissions. The ability to create shared schedules is granted to the System Administrator role by default.

To create a shared schedule, perform the following steps:

1. Open the MOM Reporting console.
2. Click on Site Settings located in the site-wide menu.
3. Click the Manage Shared Schedules link located near the bottom of the page in the Other category. From this page you can create, delete, and edit site-wide shared schedules.
4. Click the New Schedule button to display the Scheduling page, enter the name of the shared schedule and fill in the schedule details. Click OK when finished.
5. The Shared Schedules page shows the details of the schedule. Click the Home menu item to return to the Reporting console.

To use a shared schedule, start a new subscription or edit an existing subscription. In the Subscription Processing Options section of the Subscriptions page, select On a shared schedule; then choose the name of the shared schedule from the drop-down menu.

Managing Subscriptions

It is important to keep subscriptions up-to-date and edit or remove them as necessary. This avoids unnecessary accumulation of clutter on the MOM Reporting server and possibly in users' mailboxes and file servers. The Reporting console provides several ways to modify subscriptions. The first method is located on the My Subscriptions page and allows you to modify all subscriptions you've created for all reports:

1. Open the MOM Reporting console.
2. Click on My Subscriptions located in the site-wide menu.
3. A list of your subscriptions for each report is displayed. You can select the Edit button next to any of the reports to modify the details of the subscription, including the report parameters and delivery schedule.
4. To delete the subscription, check the box next to the report; then click the Delete button located on the options toolbar.

The second method allows you to view all subscriptions for a single report. Depending on your permissions level, this can also include subscriptions made by other users:

1. From within the Reporting console, open the report containing the subscriptions you want to modify.
2. After the report opens, select the Subscriptions tab.
3. A list of existing subscriptions for this report are listed. You can select the Edit button next to any of the listed reports to modify the details of the subscription, including report parameters and delivery schedule.

Managing Subscriptions

By default the Content Manager Role has the ability to view all subscriptions created by all users. This role is assigned to the local Administrators (BUILTIN\Administrators) group when the reporting server is installed.

4. To delete the subscription, check the box next to the report: then click Delete.

Customizing Report Execution, Caching, and Snapshots

Over time the MOM Reporting database can become large, and reports may take several minutes or longer to execute. Even some smaller reports seem to take a long time while you're staring at the little green "generating report" animation before the report is displayed. Several options are available to help reduce the amount of time it takes before the report is displayed on the screen.

Report Caching

Report execution can be set to cache a temporary copy after the report has been rendered the first time. This is helpful when users run reports that have selectable options. The first time a user runs a report the data is pulled from the reporting database and rendered for the user, with the resulting report kept in cache. Subsequent users who want to generate the same report can pull the data from cache when the report is executed rather than pulling the data from the reporting database, which significantly reduces the amount of time it takes the report to display on the screen. The report cache expires after a predefined number of minutes or on a shared schedule, causing the caching process to start over.

The downside to report caching is that the parameters selected must exactly match for the cache to be used, which is a potential problem because the start time and end time parameters of the report are dynamically populated when the report is opened. If the time is different even by several seconds, a new report is generated and stored in cache—eliminating the effectiveness of the caching feature. To work around this problem you can customize the report and remove hours/minutes/seconds as parameters.

Report Snapshot

Creating a report snapshot is another way to reduce the amount of time it takes to execute a report. The report snapshot function takes a snapshot of a report at a predefined time or on a predefined schedule; users running the report will look at the snapshot without needing to pull data from the reporting database every time.

The disadvantage to the report snapshot feature is that the parameters in the report must be either dynamically populated (including the start and end time of most reports) or hard-coded. When using a snapshot to view a report, none of the parameters can be changed, including the start and end time. Report snapshots are most beneficial with simple or linked reports that have the default parameters previously defined.

Report Execution

The following procedure demonstrates configuring report execution settings:

1. Open the MOM Reporting console.
2. Open the report on which you want to set the execution properties.
3. When the report opens select the Properties tab.
4. Select Execution from the properties menu on the left side of the page.
5. Configure the desired rendering and execution settings.

Both the cache and snapshot settings are useful when used correctly. Because the DTS job only updates the reporting database once a day, it is usually not necessary to generate the report from the reporting database every time.

Creating Linked Reports

The linked report capability allows you to create a linked copy of a report and then customize the parameters to suit a particular function. Linked reports can be used to provide a custom report of any performance counters MOM collects. A linked report is only a pointer to an existing report, which can pass different parameters and results for each user in a separate report with its own name.

MOM 2005 uses linked reports extensively. Reports can be generated quickly (without affecting the original report) and integrated into MOM just like other customized reports. However there are several restrictions when using linked reports:

- A linked report cannot provide reports on nonperformance counter related information.
- A linked report cannot be exported and imported into another MOM environment; it has to be manually re-created.
- Linked reports do not have the flexibility often required when building custom reports in MOM.

To demonstrate the functionality of linked reports, we will use the Performance History report located in the Microsoft Windows Base Operating System\Performance History folder. This report generates a graph with customizable performance counters from one or more servers. The disadvantage of this report is that it takes time to go through and select the parameters each time the report is to be rendered. By creating a linked report, you can hard-code the parameters for a specific set of computers into the linked copy of the report without affecting the functionality of the original report.

To create a linked report, follow these steps:

1. Open the MOM Reporting console. Open the Performance History report located in the Microsoft Windows Base Operating System\Performance History folder.
2. Select the Properties tab.
3. Click the Create Linked Report button.
4. In the Name field, type the name you want for the linked report. This name can be anything but should reflect the specific purpose of the report. This example will use the name LDAP Client Session History.
5. Optionally, click the Change Location button to create the linked report in a different directory than the original report.
6. Click OK to save the linked report. The linked copy of the report will now open to the View tab.

After creating the linked report you can customize the parameters without affecting the functionality of the original report:

1. Open the linked copy of the report if it is not already open. Select the Properties tab to view the report properties.
2. Select Parameters from the menu on the left side of the screen.
3. Uncheck the Has Default check box next to BeginDate and EndDate.
4. Check the Has Default check box next to CompGroup.
5. In the CompGroup field enter **Windows Server 2003 Domain Controllers** or **Windows 2000 Domain Controllers** depending on what type of servers you have available in your environment.
6. In the ObjName1 field enter **NTDS**.
7. In the CtrName1 field enter **LDAP Client Sessions**.
8. In the InstName1 field enter **NULL_INSTANCE**.
9. Uncheck the Prompt User check box for each parameter except for BeginDate, EndDate, and Server.
10. Click the Apply button located at the bottom of the page to save the changes. The properties should look similar to the settings in Figure 21.11.

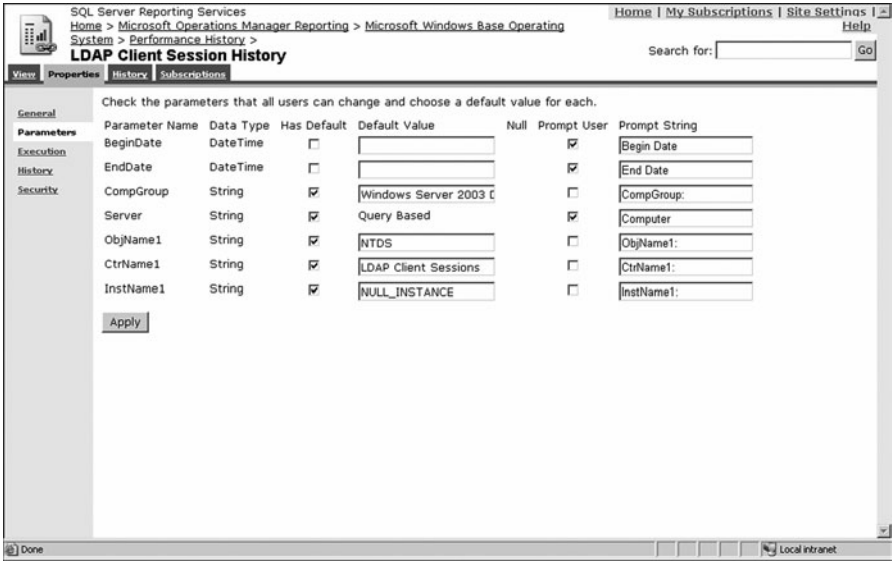


FIGURE 21.11 Linked report parameters.

Another advantage to creating a linked report is that updates to the original report are automatically reflected in all linked copies; but watch out, if the original is moved or deleted, the linked copies no longer function!

Click on the View tab to render the report. All the parameters have data in them, and all parameters except the Computer Name, Begin Date, and End Date are hidden from view. When the user runs the report, no additional data needs to be entered; the report launches automatically displaying the LDAP Client Sessions for the selected group of Windows 2000 or 2003 domain controllers over a one-week time frame.

Managing Folders and Reports

The folders and reports located on the reporting server can be easily moved or deleted in the MOM Reporting console by using the management buttons located on the button toolbar. The default buttons allow you to create new folders, create new data sources, and upload files. When the Show Details button is clicked the Move and Delete buttons are displayed, while the Contents tab shows details about each object in the folder.

Management Buttons

The following steps demonstrate how to move reports within the reporting server:

1. To show the management buttons on the toolbar, open the Reporting console and click the Show Details button located on the right side of the toolbar.
2. When the Show Details button is selected the Contents tab displays additional information beside each item within the folder and additional buttons that can be used to manage the folder contents.
3. Place a check box next to one or more items you want to move.

4. Click the Move button to display a hierarchical view of the site, click the folder you want to move your selection to, and then click OK.

Downloading Reports

If you plan to make advanced customizations to existing reports they must be downloaded from the site and added to a Visual Studio .NET 2003 report project. The following steps describe how to download and save existing reports:

1. Open the report you want to edit and select the Properties tab.
2. Click the Edit button and save the RDL file to your disk.

We will next discuss creating reports and customizing reports you have downloaded from the reporting server.

Creating Reports

A developer or report designer can use Visual Studio .NET 2003 and the SQL Server Reporting Services client components to create custom report templates. These report templates, defined with company-specific business logic, can be uploaded to the reporting server and used to render reports based on the data found in the reporting database.

Unlike the Management Pack Wizard utility included in the MOM 2005 Resource Kit, installing the Report Wizard requires several steps. The Report Wizard requires Visual Studio 2003 and other components that most organizations prefer to install on a separate report designer computer. To install the necessary software, perform the following steps:

1. On a newly built and fully patched operating system install Visual Studio 2003. Details on the installation are available in the Visual Studio .NET 2003 readme at http://go.microsoft.com/fwlink/?linkid=8861.
2. Install ASP.net.
3. Install SQL Server Reporting Services with any necessary patches.
4. Install MOM Reporting Components from the MOM 2005 installation media.

After configuring the server you can verify the wizard's functionality by opening Visual Studio 2003 (select Start, Programs, Microsoft Visual Studio .NET 2003, Microsoft Visual Studio .NET 2003) and create a new project. (Select File, New Project.) If the components were installed correctly, you will see the Business Intelligence Projects folder with the Report Project Wizard template on the right side of the screen.

An understanding or familiarity of the Transact-SQL (T-SQL) language is also beneficial but not absolutely required if you have some available time and the desire to learn. Along with the information in this chapter, the Internet offers a plethora of useful examples you can use to grow your knowledge. Microsoft provides a T-SQL guide available at http://msdn.microsoft.com/library; search on "Transact-SQL Overview."

Running Large Reports

Be cautious when developing and running reports against large amounts of data from within Visual Studio .NET 2003. By default a report run from the Visual Studio .NET 2003 Integrated Development Environment (IDE) does not operate within the same resource controls as when a report is run within SQL 2000 Reporting Services. The Visual Studio .NET 2003 IDE can easily exhaust all available resources when a report is executed against a large amount of data with a resulting significant performance degradation. It is always recommended to develop and test all custom reports in a proof of concept or development environment before implementing them in production.

MOM Reporting is a powerful feature that could easily take up an entire volume to cover each component's features and functionality. In the next section we will help you get started designing different types of reports.

Collecting Data

When developing new reports, you may find additional data needs to be captured before the report can be created. You should evaluate the impact of capturing this additional information in a proof of concept (POC) environment, testing the process and measuring the results. Your POC testing should accurately resemble what you're attempting to accomplish in production. The result of the POC can be extrapolated, and accurate predictions can be made for how much storage space is required in the reporting database for the custom data. When you experiment in a POC environment, the report and the design requirement can be evaluated and reevaluated to determine whether a more efficient method exists to collect the data or achieve the result. If your reporting database grows too quickly during the testing process, the data can simply be purged without needing to worry about the longevity of the information.

When you determine what data to collect, it is often considered more efficient from a storage perspective to capture only information you plan on using. In reality this is difficult to achieve and offers the least amount of flexibility when changes need to be made and additional information added to the report. From a reporting point of view, it is more efficient to capture the greatest amount of information possible, with near limitless reporting possibilities for your organization. By taking the lessons learned from the POC to identify report requirements, you can achieve a middle-ground approach.

Designing Reports

There are two basic methods to get the data from your reporting database when you create a report. Be cautious of how you query data from the database and take these methods into consideration when designing your business logic.

- The first method is using a simple query, getting as much data as possible out of the database without filtering or narrowing the scope. The report itself can then be used to sort and filter the data and display the correct information in the report. The downside is that this method is not the most efficient way to create simple reports

that don't have a lot of user interaction. Furthermore, in an environment with a large amount of data the report could take a long time to render.

- The second method is to design your business logic with a narrow scope, limiting the amount of data initially pulled from the database.

MOM reports are often designed with a specific purpose and a selected target, making the scope of the data narrow and able to be viewed quickly and easily. If this is the type of report you are designing, the second method is preferred when creating your business logic. If your report offers interactive functionality with user-selectable parameters, the first method may be more efficient when creating the business logic in the report. Be sure to fully test your report design before rolling it into your production environment!

A Look Inside the Reporting Database

The Reporting database consists of Dimension Tables, Fact Tables, and Periodic Snapshot Fact Tables. Each of these tables stores a specific type of data. Microsoft recommends using the corresponding views to get data from the database instead of querying the tables directly. The following examples use the SDK views. These views are specially designed to simplify the report development process by bringing together the common data required when building reports. Keep in mind that you are not limited to the SDK views when designing custom reports.

Microsoft provides detailed up-to-date documentation on all the table and view relationships available on the MOM reporting database. The SQL views for the reporting database are located within the help file, which can be downloaded with the MOM Software Development Kit at http://go.microsoft.com/fwlink/?linkid=50272. After downloading and installing the SDK file, go to Start, Programs, Microsoft Operations Manager SDK, and choose SDK Documentation. Within the SDK documentation the information is located under Microsoft Operations Manager \ MOM Reference \ MOM Data Access \ MOM Reporting Database. If you're interested, you can also dissect the SDK views using the SQL Enterprise Manager or SQL Query Analyzer (or SQL Server Management Studio for SQL Server 2005 installations) for insight on what tables are being used for each type of data collected.

Report Creation Overview

We will create two new reports to demonstrate some of the functionality available when using Visual Studio .NET 2003 with the SQL Server Reporting Services Client Components. To successfully create these reports you will need to collect specific types of data from your environment:

- Event 529—Windows security event 529 is a common event recorded in the Security event log each time a logon attempt is made with an unknown user name or a known user name with a bad password. This event is used in the first report.

- Event 531—Windows security event 531 is a common event recorded in the Security event log each time a failed logon attempt is made using a disabled account. This event is used in the first report.
- Event 624—Windows security event 624 a common event recorded in the Security event log each time a user account is added to the domain. This event is used in the second report.

Windows success and failure logging for logon events and account management needs to be enabled on the servers you want to monitor for these events, which can be accomplished by creating or modifying an Active Directory group policy. We added each of these collection event rules to a custom rule group, which was associated with all managed servers. You can limit the number of servers the custom rule group is associated with for testing purposes.

Collecting Events

The event collection rule captures the entire event each time it occurs on the target system. This may not be optimal for all environments; in a busy environment many events could be collected—resulting in large, fast database growth. The following exercises are meant as only as an example.

Creating a New Report Project

Starting a new project within Visual Studio .NET 2003 and connecting to the MOM database server is the first step in the report creation process:

Using Visual Studio .NET 2003

Do not press the F5 key. The report will *not* "refresh" the current screen as other Microsoft Windows applications do. Pressing the F5 key while in Visual Studio .NET 2003 causes the reports to be pushed or deployed to the reporting server.

1. Open Visual Studio .NET 2003 and start a new Report Project by selecting File, New, Project from the menu.
2. Select the Business Intelligence Projects type and then choose the Report Project template. Enter a project name in the field provided. This name should reflect the general category the reports within the project are targeted toward, for example, Contoso Reports. This name will reflect the folder name on the reporting server the reports are uploaded to. Click OK.
3. After the project is created, you must establish a connection to the MOM reporting database, which is done using a shared data source object. The shared data source can be added through the Solutions Explorer; if the Solution Explorer is not visible select View, Solution Explorer from the menu. Right-click the Shared Data Sources

folder within the Solution Explorer pane and select Add New Data Source. This opens the Data Link Properties window.

4. On the Connection tab of the Data Link Properties window in step 1, type in the name of the SQL Server hosting the MOM reporting database. In step 2, select Use Windows NT Integrated security for authentication. In step 3, select the MOM reporting database from the drop-down menu; by default this database is named SystemCenterReporting.
5. To verify communication to the reporting server click the Test Connection button. Click OK to acknowledge the successful connection message box. If the connection was not successful, stop and determine the cause of the communication failure before proceeding.
6. Click OK to save the configuration and close the Data Link Properties window. The new data source object is now listed under the Shared Data Sources container within the Solution Explorer.
7. Right-click on the newly crated data source and select Rename. Rename SystemCenterReporting.rds to SCDW.rds. This step is required to maintain consistency and compatibility across all reports.

Your screen should look similar to the one in Figure 21.12 with the Solution Explorer pane showing a single data source called SCDW.rds.

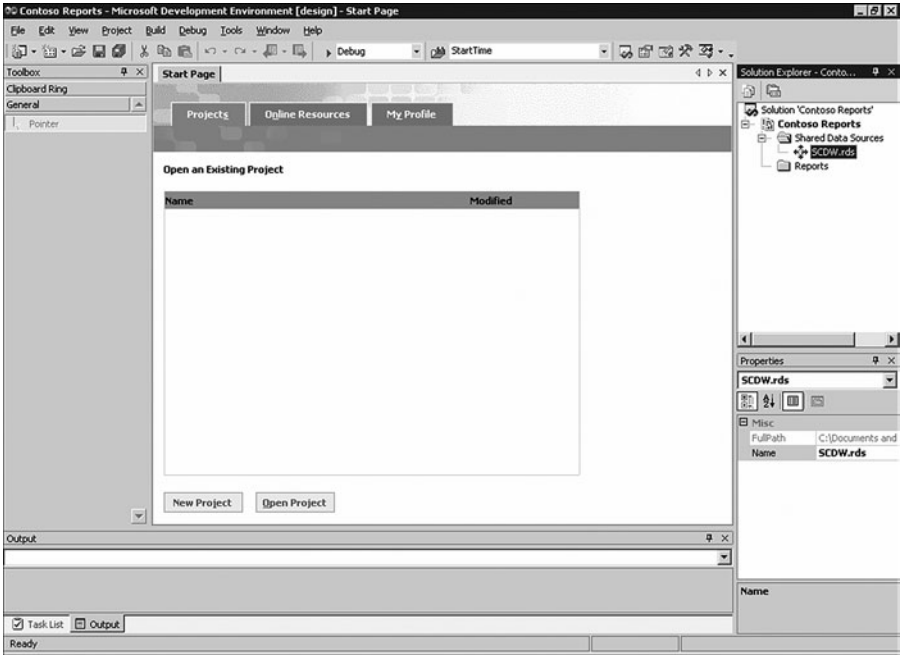


FIGURE 21.12 Solution Explorer showing the SCDW data source.

The Solution Explorer within Visual Studio .NET is the primary window used to open reports for modification. Visual Studio .NET 2003 takes up a lot of screen real-estate; if you have a small monitor you may want to hide the Solution Explorer and the Properties window when you're not using them.

Adding a Chart-Based Report to the Project

You can now add a new report to the project. This first report will display a chart showing the number of failed network logon attempts throughout the domain due to an invalid password or a disabled account. Before getting into the visual aspect of the report, let's define the logic used to retrieve data from the reporting database:

1. New reports can be added through the Solution Explorer. If the Solution Explorer is not visible, select View, Solution Explorer from the menu. From within the Solution Explorer pane, right-click the Reports folder and select Add, Add New Item to open the Add New Item window.
2. Select the Report template and enter a name for the report in the field provided. The report name should reflect the specific type of report being created—for example, Failed Logons Chart.rdl. Click Open to continue.
3. The new report is created and opened within Visual Studio .NET 2003. Select the Data tab if it has not already been selected. Select <New Dataset…> from the Dataset drop-down menu to open the Dataset properties window. Figure 21.13 shows the location of the <New Dataset…> option.

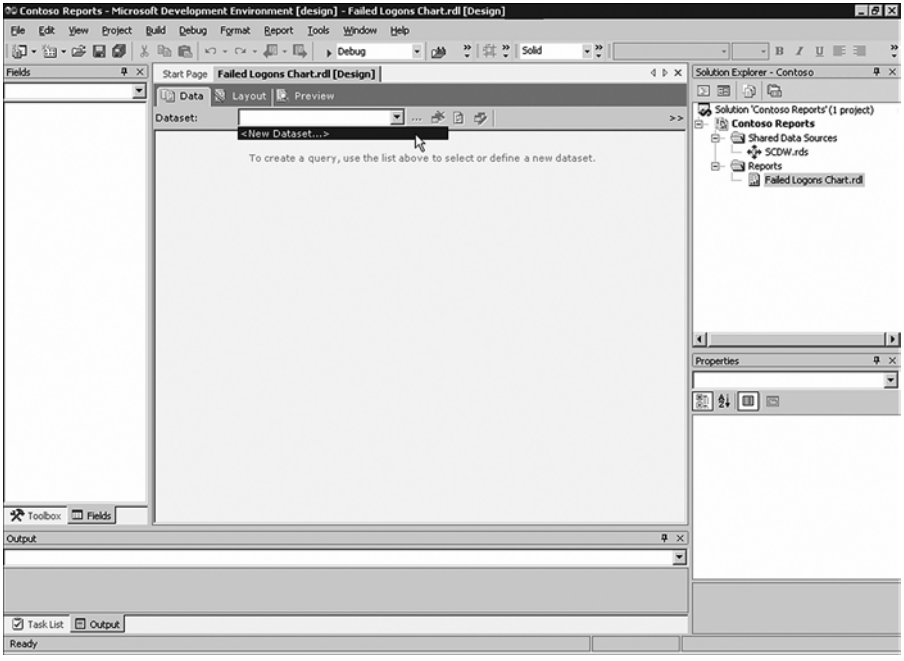


FIGURE 21.13 The New Dataset menu option on the Data tab.

4. On the Query tab, enter the name of the dataset, for example **LogonAnalysis Dataset**. Verify the SCDW data source has been selected in the Data Source drop-down menu. Click OK.

5. After the dataset is created you can add the SQL views required to obtain data from the report database. Click the Generic Query Designer button to switch to the graphical query designer view. Figure 21.14 shows the Generic Query Designer button.

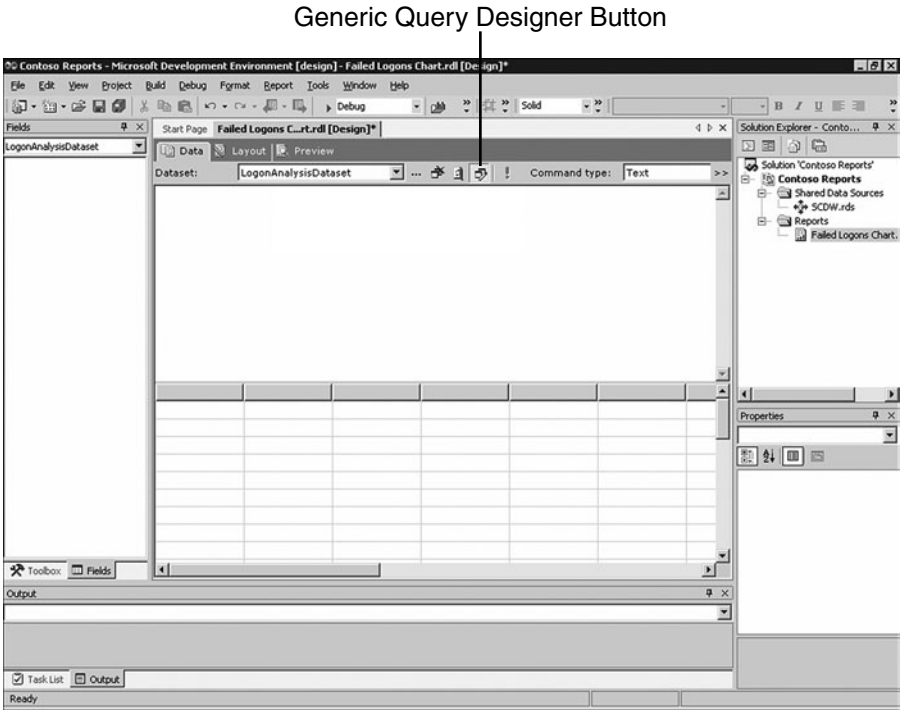


FIGURE 21.14 The Generic Query Designer button.

You can toggle between the Generic and Graphical designer view with this button.

6. Click the Add Table button, shown in Figure 21.15, to open the Add Table window. Select the Views tab; then scroll down and select SDKEventView from the list of available views. Click Add; then click Close to return to the design window. A visual representation of the view will be added to the diagram pane.

7. Scroll through the list of available column names within the SDKEventView window. Place a check next to NTEventID and TimeGenerated column names. The SQL query code in the SQL pane should look similar to the following:

```
SELECT  NTEventID, TimeGenerated
FROM    SDKEventView
```

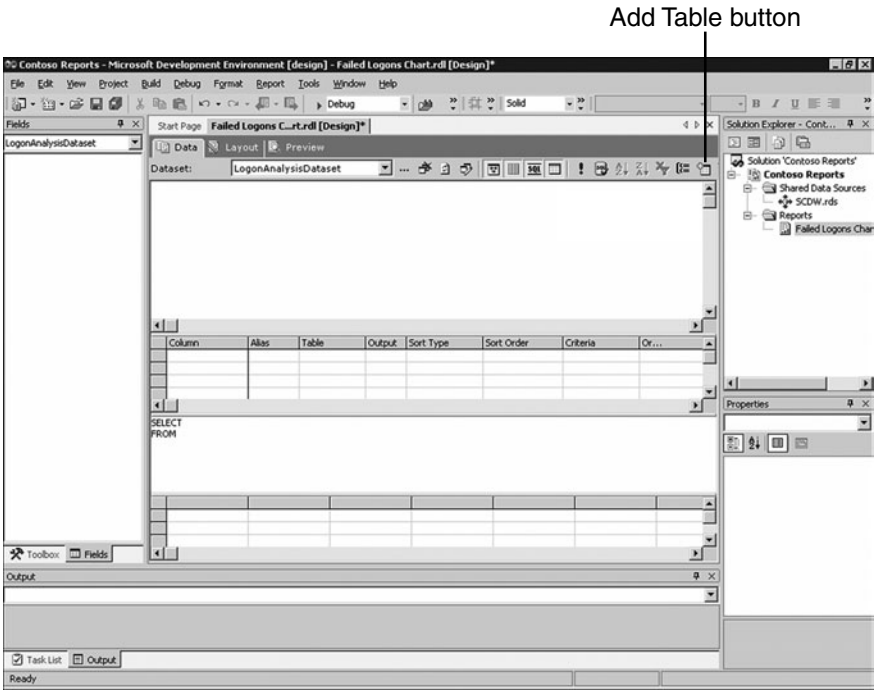


FIGURE 21.15 The Add Table button.

Defining the Business Logic

You just created a basic query. This query gathers all events from all systems in your MOM reporting database. This is a good time to save your work if you have not already done so. The next step in the process is to add some criteria to the query, narrowing the scope of data gathered. Adding criteria makes the dataset much more manageable, particularly if the reporting database is large. Remember, it is generally more important to focus the report on a specific piece or type of data, conveying a clear message to the person viewing the report.

Each of the panes within the main development window will be identified by name throughout the remaining exercises in this chapter. The name of each pane is shown in Figure 21.16.

Each pane can be toggled on or off by clicking on the corresponding button.

To create the business logic to identify the security events, take the following steps:

1. From within the Grid pane locate the NTEventID column name under the Criteria field type in **529**; then press Enter. The code within the SQL pane should now look similar to the following. The changes are highlighted in bold.

```
SELECT  NTEventID, TimeGenerated
FROM    SDKEventView
WHERE   (NTEventID = 529)
```

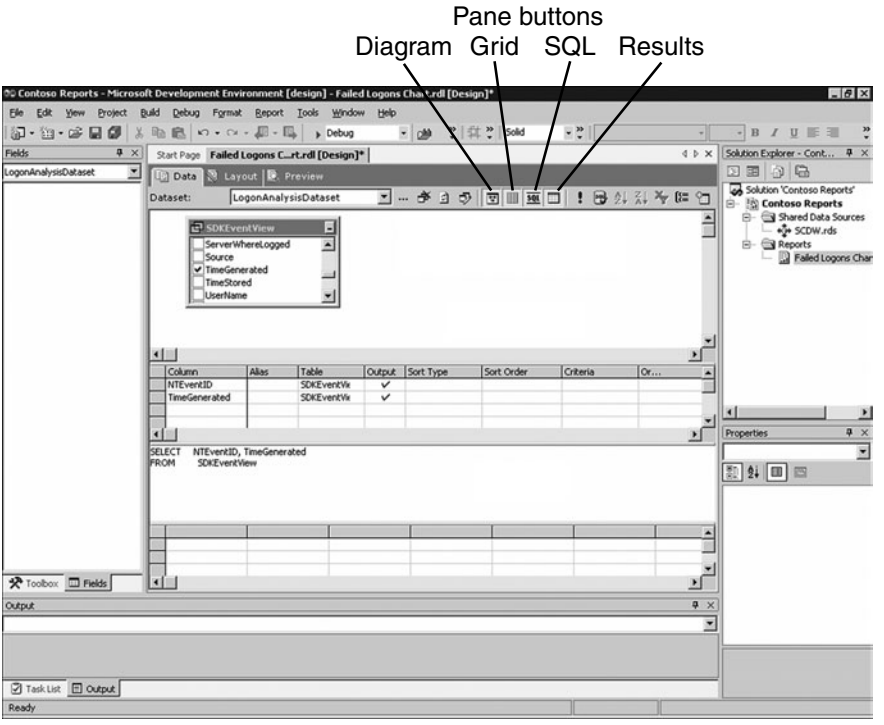


FIGURE 21.16 Panes available within the Graphical Design view.

Always Test Your Queries

The preceding query is basic. If run against a large database this query could consume a lot of resources on the development system and/or reporting server. It is always recommended to develop reports in a proof of concept environment first before running custom reports against your production database.

2. Click the Run button. The Results pane will list each occurrence of event 529. Windows security event 529 is a common event recorded on a server each time a logon attempt is made with an unknown user name or with a known user name having a bad password.

3. Additional events can be collected by adding values to one or more of the available Or fields. For example you may want to expand the scope to include security event 531, failed logon attempts made using a disabled account. Type **531** in the first available Or field for the NTEventID column name; then press Enter. The query will now list occurrences of the events 529 and 531.

   This chart only needs to display the count of each event, not each individual occurrence. One way to get the count of each event is by adding a column that adds up each occurrence of each event. This can be done with the Grid pane.

4. Select NTEventID from the drop-down menu in an empty column field.
5. In the Alias field type **EventCount**.
6. In the Group By field select Count from the drop-down menu.
7. Make sure that the Output field is checked.

   The code within the SQL pane now looks similar to the following. The changes are highlighted in bold.

```
SELECT NTEventID, TimeGenerated, COUNT(NTEventID) AS EventCount
FROM SDKEventView
GROUP BY NTEventID, TimeGenerated
HAVING (NTEventID = 529) OR
       (NTEventID = 531)
```

   When you execute the code, many events are still displayed in the Results pane, and the newly created EventCount field only displays 1 or 2 occurrences. This is because the events are grouped by NTEventID and TimeGenerated and because the value in the TimeGenerated field is accurate to within 1 second. Only the events occurring within the same second are grouped together. We next change the TimeGenerated value so that the grouping of events occurs over a full day:

8. To change the report so that the event count is based on the entire day, first remove the TimeGenerated column from the query. This is done within the Diagram pane; scroll down and remove the check next to the TimeGenerated column name.
9. From within the Grid pane add a new column by typing **CONVERT(char(10), TimeGenerated, 101)** in the first available cell after the last column name. Change the alias to EventDate. Now when the query is executed the count of events is based on the Day/Month/Year, effectively excluding the hours, minutes, and seconds from the calculation. The code within the SQL pane should look similar to the following. The changes to the code are highlighted in bold.

```
SELECT NTEventID, COUNT(NTEventID) AS EventCount,
       CONVERT(char(10), TimeGenerated, 101) AS EventDate
FROM SDKEventView
GROUP BY NTEventID, CONVERT(char(10), TimeGenerated, 101)
HAVING (NTEventID = 529) OR
       (NTEventID = 531)
```

   In this example the CONVERT function is used to change the style of the TimeGenerated value to the Month/Day/Year format. You can consult a T-SQL language reference for additional information on the CONVERT function.

10. When the query is executed the Results pane will list how many times each event occurred over the course of each day. At this time you may notice the date listed in the EventDate column is not sorted correctly. From within the Grid pane, select 1 from the drop-down menu in the Sort Order field of the CONVERT(char(10), TimeGenerated, 101) column name. The sort type field will now display Ascending.

The code within the SQL pane should look similar to the following. The changes to the code are highlighted in bold.

```
SELECT NTEventID, COUNT(NTEventID) AS EventCount,
       CONVERT(char(10), TimeGenerated, 101) AS EventDate
FROM SDKEventView
GROUP BY NTEventID, CONVERT(char(10), TimeGenerated, 101)
HAVING (NTEventID = 529) OR
       (NTEventID = 531)
ORDER BY CONVERT(char(10), TimeGenerated, 101)
```

Adding the Graph

After defining the business logic, the next step in the process is to add the visual aspect of the report. In our example a graph is displayed representing failed logon attempts due to bad passwords or disabled user accounts.

Follow these steps to add a graph:

1. Select the Layout tab. Right-click on the body of the report and select Properties. Figure 21.17 shows the Properties pane.

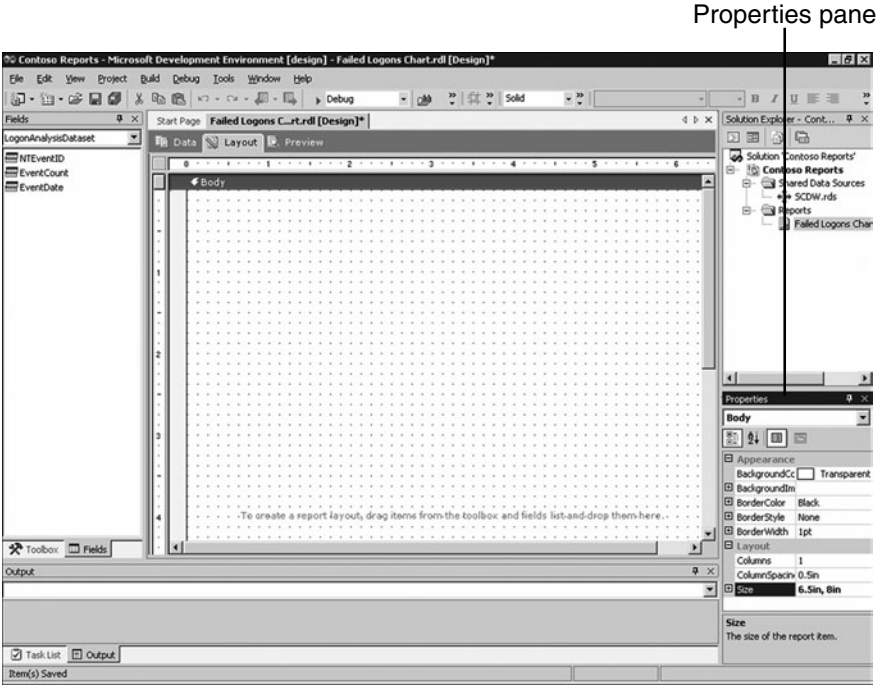


FIGURE 21.17 The Properties pane.

The Properties pane will show the properties for the currently selected area or item. Figure 21.17 shows the properties of the Body as shown in the drop-down menu just below the pane title.

2. In the Properties pane change the Size of the report body to 6.5in, 8in.
3. Select View, Toolbox from the menu to display the tools quick menu, as shown in Figure 21.18. Drag the Chart icon to the body of the report. Resize the chart to fit within the body of the report. Remember to leave enough room for additional report elements such as the title, description, and any graphics you may want to add to the report.

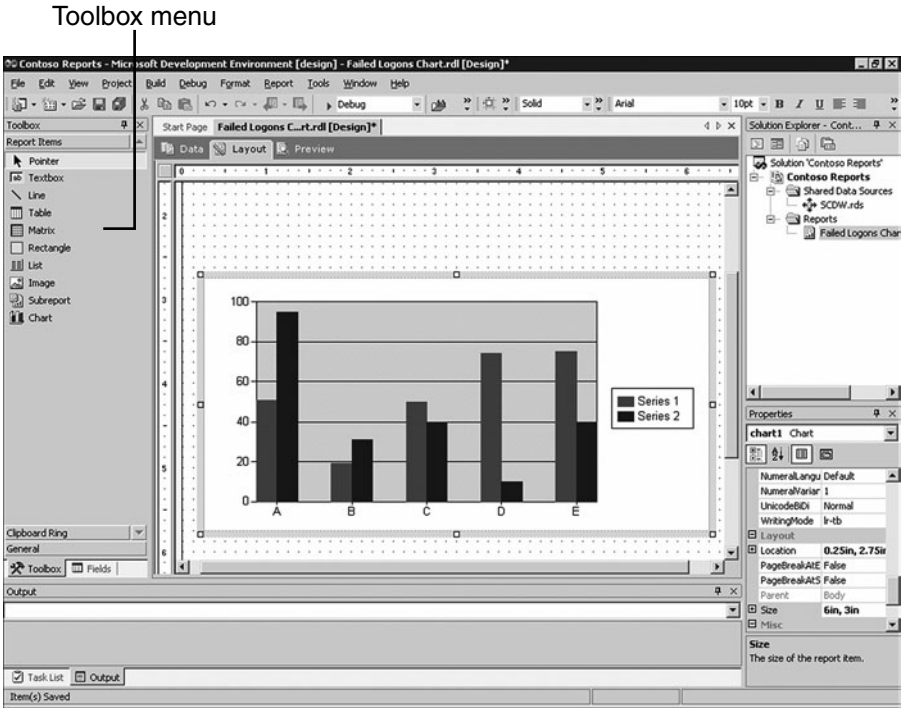


FIGURE 21.18 The Toolbox menu.

4. Right-click the Chart and select Properties. The Chart Properties window will open. This properties window offers a different set of customizable properties than the Properties pane.
5. On the General tab, select Column from the Chart Type list. Select the Legend tab and click the bottom middle box to reposition the chart legend, as shown in Figure 21.19. Click OK to close the properties window.
6. Select View, Fields from the menu to display the Fields quick menu.
7. Double-click the chart to display the field placeholders for each axis.
8. Drag the EventCount field to the data area at the top of the chart.
9. Drag EventDate to the category area at the bottom of the chart.
10. Drag NTEventID to the series area on the right side of the chart.

The chart in your report should now look similar to the one in Figure 21.20.

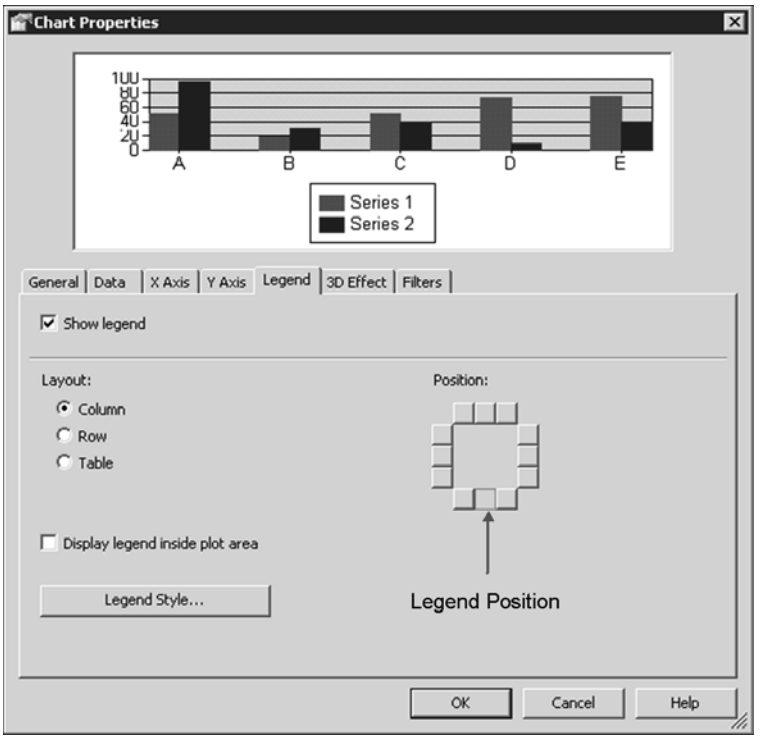


FIGURE 21.19 Chart properties.

Adding Interactive Parameters

You can easily add user interactive parameters to a report template. This is useful when packaging the template for redistribution or when the report requirements frequently change. By adding parameters the user can customize data in the report before the report is rendered. These parameters can be added in a way to automatically provide the suggested default, or prevent the user from selecting anything except values from the given list.

One of the most common parameters that should be considered for all reports is a date range. The default retention time for the MOM reporting database is 395 days. As the database grows, a report based on all the data takes longer and longer to execute, potentially exceeding the execution time threshold and causing the report to fail. It is more efficient to add a date scope for your report, limiting the time frame the report is based on.

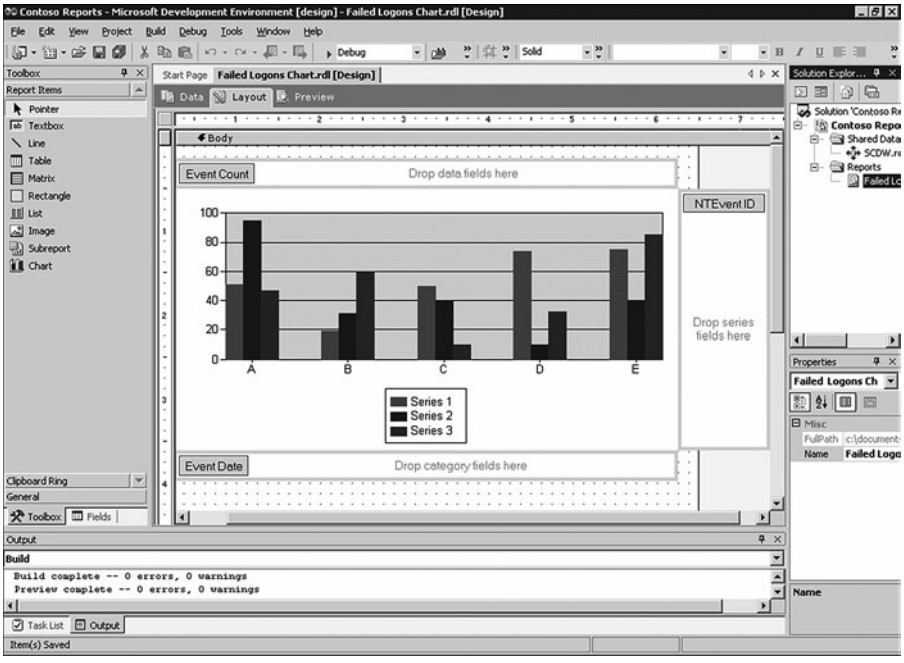


FIGURE 21.20 Chart data field placement.

To limit the date range for our report we perform the following steps:

1. Select the Data tab.
2. From within the Grid pane, locate the NTEventID column name that contains the Criteria value of = 529 and Or… value of = 531. Remove the value = 531 from the Or… field and change the Criteria field to = 529 OR 531. This change is important because it tells the server to get data from both events only if they were created between the Start and End time.
3. Within the Grid pane, locate the CONVERT (char(10), TimeGenerated, 101) column name. In the Criteria field type **BETWEEN @StartTime AND @EndTime**; then press Enter. The code within the SQL pane should look similar to the following. The changes to the code are highlighted in bold.

```
SELECT  NTEventID, COUNT(NTEventID) AS EventCount,
        CONVERT(char(10), TimeGenerated, 101) AS EventDate
FROM  SDKEventView
GROUP BY  NTEventID, CONVERT(char(10), TimeGenerated, 101)
HAVING  (NTEventID = 529 OR NTEventID = 531) AND
        (CONVERT(char(10), TimeGenerated, 101)
          BETWEEN @StartTime AND @EndTime)
ORDER BY CONVERT(char(10), TimeGenerated, 101)
```

The @StartTime and @EndTime within the SQL query are used to define parameters. These parameters can be named anything you want but should reflect their general purpose and need to be prefixed with the @ symbol. When the report is run the server notices that additional parameters are needed; because these parameters affect how the report is displayed, the report cannot be generated without this information. SQL Server Reporting Services automatically identifies the parameters that need additional input and generates an area above the report with the appropriate fields for the user to enter values.

By clicking the Preview tab, you'll notice that the area above the report was added with two fields labeled StartTime and EndTime. These fields allow you to enter values that control the time frame the data in the report is sampled on.

Introducing parameters creates an additional problem. The viewer of the report needs to know how to enter the appropriate information to get the correct data; in this case the user will have to know the correct date format of the start and end time. To address this problem we can add default values to the StartTime and EndTime parameters.

Adding default values to report parameters is a straightforward process and can be accomplished in several ways. You could simply type in the default values, but the viewer would have to change the parameters each time he ran the report. We can also add dynamic values to the parameters starting with a set number of days before the current date in the StartTime parameter and ending with the current date in the EndTime parameter.

To dynamically set the value of parameters in the report we'll add a new dataset. This dataset will be used to generate a date range using a predefined function. Follow these steps:

1. Select the Data tab.
2. Select <New Dataset…> from the Dataset drop-down list. The Dataset Properties window is displayed.
3. On the Query tab enter the name of the dataset—for example, DateRangeDataset. Click OK.
4. Select the Generic Query Designer button to change back to the graphical designer view.
5. Click the Add Table button to open the Add Table window.
6. Select the Functions tab, scroll down, and select fn_GetDateRange from the list of available functions. Click Add; then click Close to return to the design window.
7. Place a check next to the top column, * (All Columns).
8. In the SQL Pane add the number **7** between the brackets of the function. The code should look similar to the following. The changes are highlighted in bold.

```
SELECT fn_GetDateRange.*
FROM   fn_GetDateRange(7) fn_GetDateRange
```

9. Click the Run button. The Results pane should display a BeginDate and an EndDate, with the begin date 7 days earlier than the end date.

Now we have a dataset that gets the date range. The next step is to add this date range as the default values for the report parameters. We will specify both a BeginDate and an EndDate:

1. Select Report, Report Parameters from the menu to open the Report Parameters properties window.
2. Select StartTime from the Parameters list on the left side of the window.
3. Set the Default Values radio button to From Query.
4. Select the DateRangeDataset from the Dataset drop-down menu.
5. Select the BeginDate from the Value field drop-down menu.
6. Select EndTime from the Parameters list on the left side.
7. Set the Default Values radio button to From Query.
8. Select the DateRangeDataset from the Dataset drop-down menu.
9. Select the EndDate from the Value field drop-down menu. Click OK.

You can now click the Preview tab. The report server will now render the report automatically, using the dynamic default values provided.

Adding the Company Logo

You may have noticed the report is missing some details such as the company logo. Adding a company logo to a report is simple. In this procedure we will show how to embed the image in the report. In the next report we'll look at how to add the image as part of the project. Follow these steps to embed the image:

1. Select Report, Embedded Images from the menu to open the Embedded Images dialog box.
2. Select the New Image button, browse to the location of the logo you want to embed in the report, select the logo, and click the Open button.
3. Click OK to close the Embedded Images dialog box.
4. Select the Layout tab.
5. Select Report, Page Header to display the header above the report body.
6. Select View, Toolbox from the menu.
7. Drag the Image icon from the toolbox to an area in the page header. This will open the Image Wizard. Click Next.
8. On the Image Source Page select Embedded. Click Next.
9. On the Choose Embedded Image page, select your logo that was just uploaded. Click Next and then click Finish to complete the wizard.

10. Resize the image to fit within the desired header area. Resize the header by dragging the Body separator bar to the desired position.

The image will be placed in the header of each report. If the report spans multiple pages, the logo displays on the top of each page. Feel free to move and position the logo to where it looks visually appealing. You can also add text boxes and additional images to the report such as the company name, a report title, a detailed description of the report, and possibly some footer data.

Adding a Tabular-Based Report to the Project

We will now add a second report to the project. This report will display a tabular data view showing account management throughout the entire domain. One of the nice features of a tabular style report is the ability to expand and collapse different "groups" of data, allowing the viewer to control the amount of information displayed on the screen. This report will be created using the Report Wizard to take advantage of some of the built-in user-friendly features available when creating tabular style reports. Follow these steps:

1. Open your report project. From within the Solution Explorer, right-click Reports and select Add New Report to open the Report Wizard Welcome page. Click Next.
2. On the Select the Data Source page, select the SCDW data source created when the project was established and click Next.
3. On the Design the Query page, select Edit to open the Query Builder. Maximize the Query Builder window.
4. Right-click anywhere within the top Diagram pane and select Add Table to open the Add Table dialog box.
5. Select the Views tab, scroll down, and select SDKEventView from the list of available views. Click Add; then click Close to return to the Query Builder.
6. Place a check next to the ComputerName, Message, NTEventID, and TimeGenerated column names; click OK to close the Query Builder window. Click Next.
7. On the Select the Report Type page, enable the Tabular radio option. Click Next.
8. On the Design the Table page, highlight the ComputerName and NTEventID fields from within the Available Fields list. Click the Group button to add these fields to the Group display area. Verify that ComputerName is listed before NTEventID field. You can use the Up/Down arrows to change the order of the fields.
9. Highlight the TimeGenerated and Message fields from within the Available Fields list. Click the Details button to add these fields to the Details display area. Make sure that TimeGenerated is listed before the Message field. Use the Up/Down arrows to change the order of the fields. Click Next.
10. On the Choose the Table Layout page, leave the Stepped option selected and place a check next to the Enable Drilldown option. Click Next.

11. On the Choose the Table Style page, select Corporate. Click Next.
12. On the Completion page, enter a name for the report in the field provided—for example, **Account Management Report**. Click Finish.

A new report is created that displays the selected fields in a tabular format. One of the nice features of the Report Wizard is its capability to create the drill-down tabular report by simply selecting the location of the parameters. The wizard automatically creates the table and the correct table groups. You can view how the table groups are created by clicking in one of the table cells; the table properties frame will appear around the table, as shown in Figure 21.21. Right-click on one of the table groups and select Edit Group to open the Grouping and Sorting window. You can see some of the customization required to give the table the capability to expand and collapse.

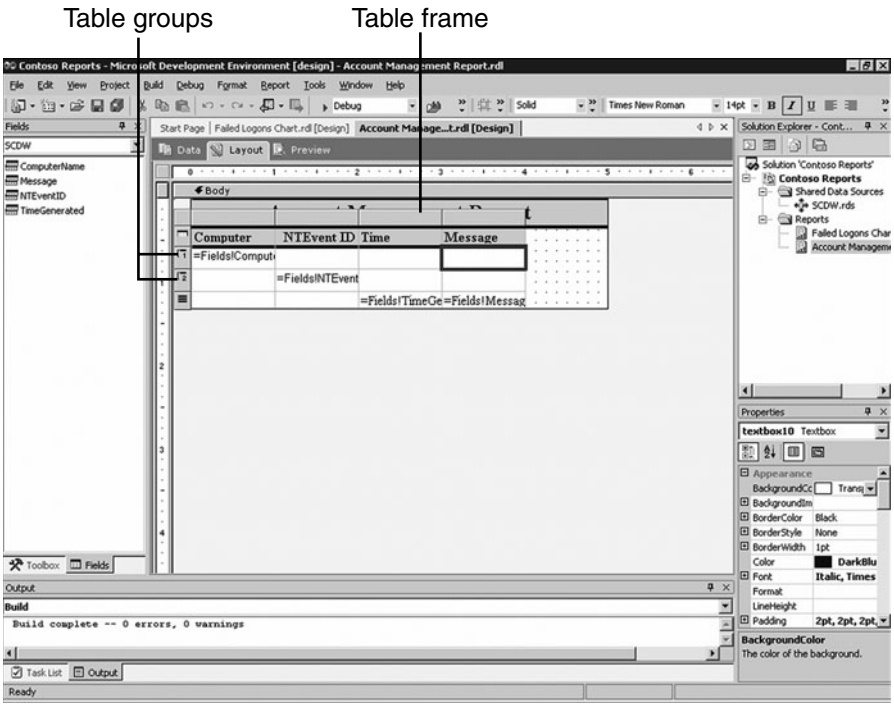


FIGURE 21.21 The Table Properties frame.

Defining the Business Logic

The next step in the process is defining the business logic. We previously added a table and selected the column names we wanted for our report. To make the report more effective we will reduce the amount of data, targeting a specific purpose. This report is going to show all the accounts that have been added to the domain:

1. Select the Data tab, find the NTEventID column name, and enter **624** in the Criteria field.

2. Click the Preview tab; the report will show information about all user accounts that have been added to the domain.

   The "expand" and "collapse" icons on the left side of each group allow the user to control how much information is displayed. You may notice a large amount of data in the Message field of the report. The information in the Message field can also be filtered, effectively reducing the amount of noise in the report.

3. Select the Data tab; then click the Add Table button.

4. Select the Views tab, scroll down, and select SDKEventParametersView from the list of available views. Click Add; then click Close to return to the report designer.

5. You will now see two tables in the Diagram pane. The first table contains basic event data, and the second table contains the data contained in each parameter of the event. To join these tables together drag the column name EventGUID from the first table and drop it on the EventGUID column name in the second table. A link between the two tables will be created, as shown in Figure 21.22 indicating the tables have been joined.

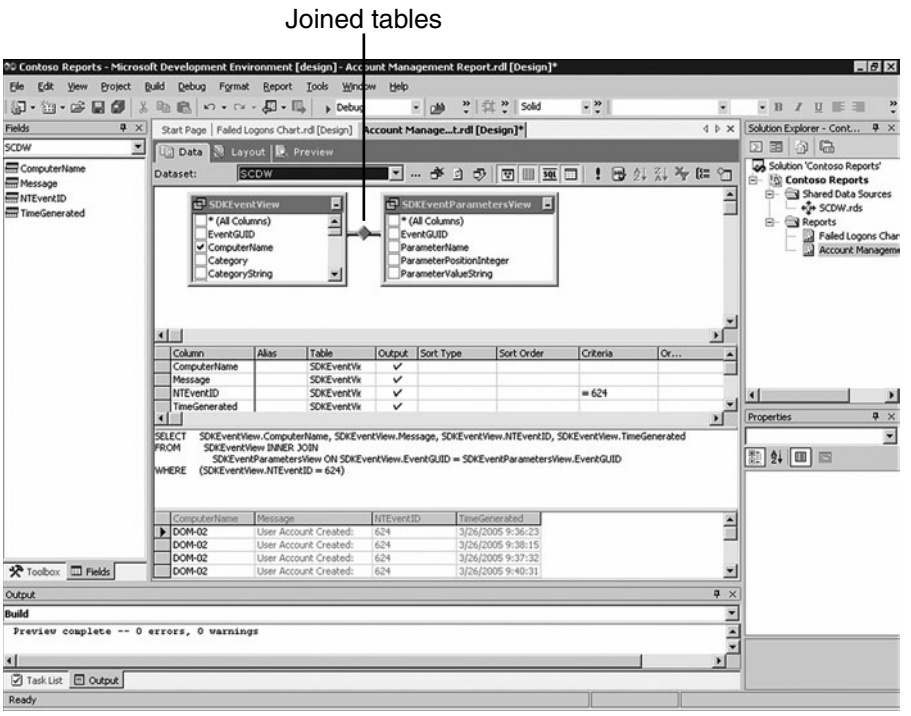


FIGURE 21.22 Joined tables.

When tables are joined, data from each table can be selected as if it were part of the same row of data. For the join to work correctly both tables must have a common column. For this example the column EventGUID is the same in both tables.

6. In the table SDKEventView uncheck the column name Message. In the table SDKEventParametersView check the box next to the ParameterValuePositionInteger and ParameterValueString columns.
7. Select the Layout tab, right-click the Message text box cell and select Properties to open the Textbox Properties window.
8. Change the Value field from =Fields!Message.Value to =Fields!ParameterValueString.Value by choosing the correct formula from the drop-down list. Click OK.

   The report will now list all the parameters individually instead of the entire event message. The next step is to filter the parameters you don't want. Normally this step would take additional research to determine the value of each parameter. You can obtain documentation from Microsoft regarding the Windows security event parameters by searching for "Windows Server 2003 Security Guide" at http://www.microsoft.com/downloads.
9. Select the Data tab, locate the ParameterPositionInteger column name and enter **1 OR 2 OR 4 OR 5** in the Criteria field. This will tell the report that we only want parameters in specific positions. These positions will show the account and domain of the user that was created and the account and domain of the administrator that added the account.

Event Parameters

Windows 2000 and 2003 have many parameters that can be selected, and not all the parameters are in the same position for each event. For additional information on the parameter values review the event collected through the MOM Operator console or the Windows Server 2003 Security Guide discussed in step 8.

10. Select the Preview tab to view the report. The report will now display the name of the user account that was created, the name of the domain the user was created in, and the name of the administrator account and domain the new user was created from.

The report should look similar to the one in Figure 21.23.

Defining the Report Layout

You may have noticed several items that should be fixed, such as the time value next to each of the parameters and the fact that the parameters don't have descriptions associated with them. To add the time value to the report layout, perform the following steps:

1. Select the Layout tab and select the cell that contains the time generated value. This should be listed as =Fields!TimeGenerated.Value. Right-click and select Properties to open the Properties window for this cell.
2. Check the Hide Duplicates check box and select SCDW from the Containing group or Dataset drop-down menu. Click OK to close the window.

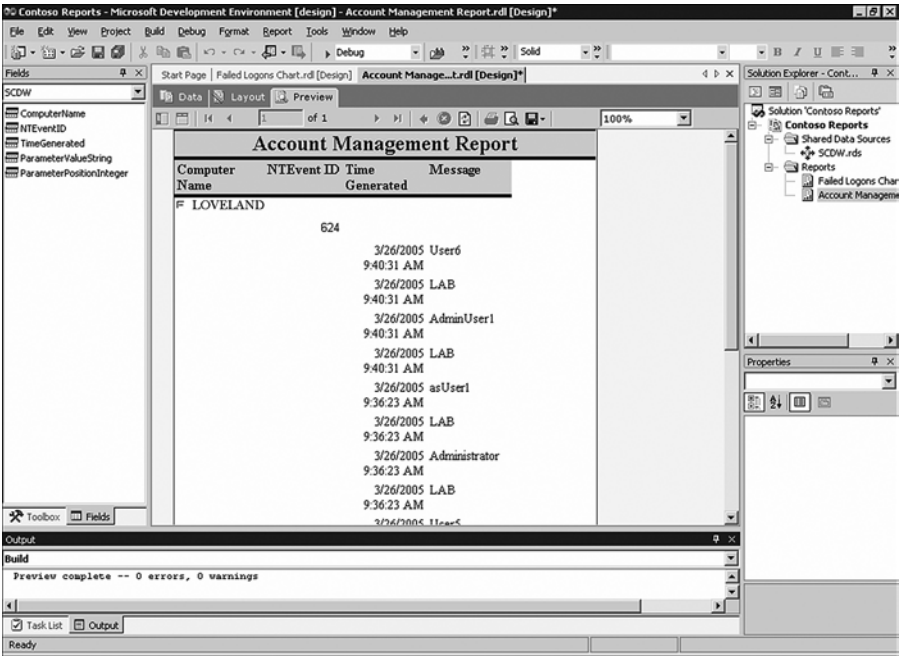


FIGURE 21.23 Account Management report.

3. Select the Preview tab. The report will now display the time value once for each event listed.

Now we will add descriptions beside the column names:

1. Select the Layout tab. Click on any cell within the table to show the table properties border. Right-click on the area above the Message column and select Insert Column to the Left.
2. In the newly created column, select the cell on the same row as where the message is displayed. Right-click the cell and select Properties.
3. In the Value field type the following code within the value field. Note that the code has been "wrapped" for readability, this code should be typed in as a single line in the value field.

```
=Switch(Fields!ParameterPositionInteger.Value=1, "User Name: ",
Fields!ParameterPositionInteger.Value=2, "User Domain: ",
Fields!ParameterPositionInteger.Value=4, "Created by: ",
Fields!ParameterPositionInteger.Value=5, "From Domain: ")
```

The code evaluates the Parameter position and changes the text displayed in the field accordingly. Now when you select the Preview tab, the report displays a description beside each of the parameters in your report.

Adding Interactive Parameters

In this report we'll add the same StartDate and EndDate parameters to narrow the scope of the report. Follow these steps:

1. Select the Data tab.
2. From within the Grid pane, locate the TimeGenerated column name.
3. In the Criteria field type **BETWEEN @StartTime AND @EndTime**. The code within the SQL pane should look similar to the following. Changes to the code are highlighted in bold.

```
SELECT SDKEventView.ComputerName, SDKEventView.Message,
       SDKEventView.NTEventID, SDKEventView.TimeGenerated,
       SDKEventParametersView.ParameterPositionInteger,
       SDKEventParametersView.ParameterValueString
FROM SDKEventView INNER JOIN
     SDKEventParametersView ON SDKEventView.EventGUID =
     SDKEventParametersView.EventGUID
WHERE (SDKEventView.NTEventID = 624) AND
      (SDKEventParametersView.ParameterPositionInteger = 1 OR
       SDKEventParametersView.ParameterPositionInteger = 2 OR
       SDKEventParametersView.ParameterPositionInteger = 4 OR
       SDKEventParametersView.ParameterPositionInteger = 5) AND
    (SDKEventView.TimeGenerated BETWEEN @StartTime AND @EndTime)
```

Next we will add default values to the report parameters to assist the person viewing the report:

1. Select the Data tab.
2. Select <New Dataset…> from the Dataset drop-down list. The Dataset properties window will be displayed.
3. On the Query tab enter the name of the dataset—for example, enter DateRangeDataset. Click OK.
4. Select the Generic Query Designer button to change back to the graphical design view.
5. Click the Add Table button to open the Add Table window.
6. Select the Functions tab, scroll down, and select fn_GetDateRange from the list of available functions. Click Add; then click Close to return to the design window.
7. Place a check next to the top column, * (All Columns).
8. In the SQL pane add the number **30** between the brackets of the function. The code should look similar to the following. The changes are highlighted in bold.

```
SELECT fn_GetDateRange.*
FROM   fn_GetDateRange(30) fn_GetDateRange
```

9. Select the Run button. The Results pane should display a BeginData and an EndDate; the begin date should be 30 days earlier than the end date.

We now have a dataset that gets a range of dates. The next step is to add this date range as default values for the report parameters:

1. Select Report, Report Parameters from the menu to open the Report Parameters properties window.
2. From the Parameters list on the left side select StartTime.
3. Set the Default Values radio button to From Query.
4. Select the DateRangeDataset from the Dataset drop-down menu.
5. Select the BeginDate from the Value field drop-down menu.
6. From the Parameters list on the left side select EndTime.
7. Set the Default Values radio button to From Query.
8. Select the DateRangeDataset from the Dataset drop-down menu.
9. Select the EndDate from the Value field drop-down menu. Click OK.

Click the Preview tab to view the report. The report automatically launches because we added default values to the parameter list.

Adding the Company Logo

We can add the company logo to the report. This time we will add the logo to the report project and upload it to the reporting server. The advantage to adding the graphic to the project is that the logo can be updated in a central point, without having to modify and republish each individual report if the logo changes. Follow these steps to add the logo:

1. Select the Layout tab and select Report, Page header from the menu to show the report header.
2. Select View, Toolbox from the menu to show the toolbox menu list. Drag and drop the image icon onto the header area of the report. The Image Wizard will open. Click Next.
3. On the Select the Image Source page, click the Project radio button.
4. On the Choose the Image from the Project page, click the New Image button; then browse and select the company logo. Click Open to add the logo to the project. Click Next.
5. On the Completion page, a preview of the image will be shown. Verify the image and then click Finish to close the window.
6. Resize the image by dragging the control nodes on the image or by specifying the dimensions in the Properties pane. You can view the Properties pane of the image

by right-clicking the image and selecting Properties and then looking for the Size property.

Alternatively you can create linked images in your reports by specifying the URL of the graphic file on a web server. This option is useful if your company already has a common web server that stores this type of data.

Additional Modifications

Within Visual Studio .NET you can make a limitless number of customizations to the report and the layout. Customizations can include features such as alternating the color of table rows, highlighting values that reach or exceed a specific threshold, or anything else you can think of. Our previous examples demonstrated the basic design of several report types. We recommend that you keep working with the reports and explore the many other different options available. Also note that SQL Server Reporting Services comes with a sample database and several sample reports you can use to learn other customization techniques.

Modifying an Existing Report

The preceding examples demonstrated how to start a new project and create new reports from the ground up. The next example adds an existing report to your report project and then makes some modifications to suit a specific purpose. You will often find it is more efficient to make small modifications to an existing report that provides similar functionality than to start from scratch each time. A good candidate for customization is the Performance Analysis report, found in the Operational Health Analysis folder. This report is automatically uploaded to the reporting server when MOM Reporting is installed and offers an extensive amount of potential due to its generic structure.

The first step is to download the report from the reporting server and add it to your existing report project:

1. Open the Performance Analysis report located in the Operational Health Analysis folder.
2. After the report opens, click the Properties tab.
3. Click the Edit link located under the Report Definitions area. A download will open. Save the Performance Analysis.RDL file to the local computer.
4. Open Visual Studio .NET 2003 and then open the report project that was created earlier in the section “Creating a New Report Project.”
5. From within the Solution Explorer pane, right-click Reports and select Add, Add Existing Item.
6. Browse to the location of the Performance Analysis.RDL file that was downloaded from the reporting server. Select the file and click Open.
7. The Performance Analysis report will be added to the list of reports displayed in the Solution Explorer for your project.

This particular report is useful because it already contains logic used to retrieve the average performance data from up to four different performance counters over a 1-hour period. The main drawback to this report is that you can only select a single computer. The following modification changes the report so that data can be collected from an entire group of computers. This is useful when you want to compare trends of similar types of systems on the same chart. This example charts the processor performance of domain controllers. If you have many domain controllers you may want to narrow the criteria to a single site. Perform the following steps:

1. Right-click the Performance Analysis.RDL report within the Solution Explorer and select Open.
2. When the report opens select the Data tab.
3. Select the ComputerList dataset from the Dataset drop-down menu.
4. Modify the existing code to look like the following; the changes are highlighted.

```
SELECT  Computer as Server
FROM  dbo.fn_GetComputerIDsInGroup(@CompGroup)
UNION
SELECT '<ALL>'
order by Server
```

The next modification can be used to hard-code parameters in the report and hide them from the user's view. You can achieve a similar result by creating a linked copy of the report and then hard-coding and hiding the values directly through the MOM Reporting console. The drawback to modifying the report through the Reporting console is that the report graph will always show four performance sets even if you want the report to display a only single counter. So for this example we will modify the report directly. Follow these steps:

1. Select Report, Report Parameters from the menu.
2. Select CompGroup from the parameters list, set the Default values section to Non-queried and then enter **Windows Server 2003 Domain Controllers** or **Windows 2000 Domain Controllers**, depending on the servers available in your environment.
3. Select ObjName1 from the parameters list, set the Default values section to Non-queried, and then enter **Processor** in the field provided.
4. Select CtrName1 from the parameters list, set the Default values section to Non-queried, and then enter **% Processor Time** in the field provided.
5. Select InstName1 from the parameters list, set the Default values section to Non-queried, and then enter **_Total** in the field provided.
6. Select ObjName1 from the parameters list, set the Default values section to Non-queried, and then enter **Processor** in the field provided.

The next step removes the parameters from the user's view. By removing or showing the parameters required to run the report you can control the focus of the report.

7. With the Report Parameters window still opened, select each parameter in the parameters list and remove the value in the Prompt field.
8. Click OK to close the window and save the settings.

The report has now been configured to display the % Processor time for all domain controllers. If you have many domain controllers you may want to enter a custom group with a limited number of servers to avoid overloading the chart with data. We now will remove the extra performance data from the chart:

1. Select the Layout tab.
2. Double-click on the chart to display each set of fields in a frame around the chart. The data fields along the top of the chart should be listed in boxes called Average Performance 1, Average Performance 2, Average Performance 3, and Average Performance 4.
3. Remove the Average Performance 2, 3, and 4 data field boxes from the chart by right-clicking each box and selecting Delete.

When this report is run, a graph is automatically generated displaying the average processor performance history for all domain controllers over a one-week time frame. If the chart is too cluttered the domain controllers can be grouped and individual reports created for each group.

Additional customization can be made to the report; for example, you may want to monitor several performance counters on a group of servers. From the Layout tab of the report you can copy and paste the entire chart to make one or more duplicates. On the first copy of the chart you can display the Average Performance 1 data field, on the second copy of the chart you can display the Average Performance 2 data field, and so on. This is beneficial when you want to monitor several performance counters on a group of servers, such as the mail queue lengths, disk latency, and processor time for a group of Exchange servers.

Publishing Your Report

After creating and testing your reports they are ready to be published to the MOM reporting server. In most cases you are developing in your POC environment so you will publish to the POC MOM reporting server. After testing the new and custom reports in your POC environment you can move them into production:

1. From within the Solution Explorer right-click on the project and select Properties. Enter the project name. In this case our project is called **Contoso Reports**.

2. On the Properties page, change the TargetFolder field to **Microsoft Operations Manager Reporting/Contoso Reports**. This is the folder that will be created within the MOM reporting server.
3. Change the TargetServerURL field to the URL of the report server—for example, **http://<*server name*>/ReportServer**. The Reports Property Pages windows should look similar to Figure 21.24. Click OK.

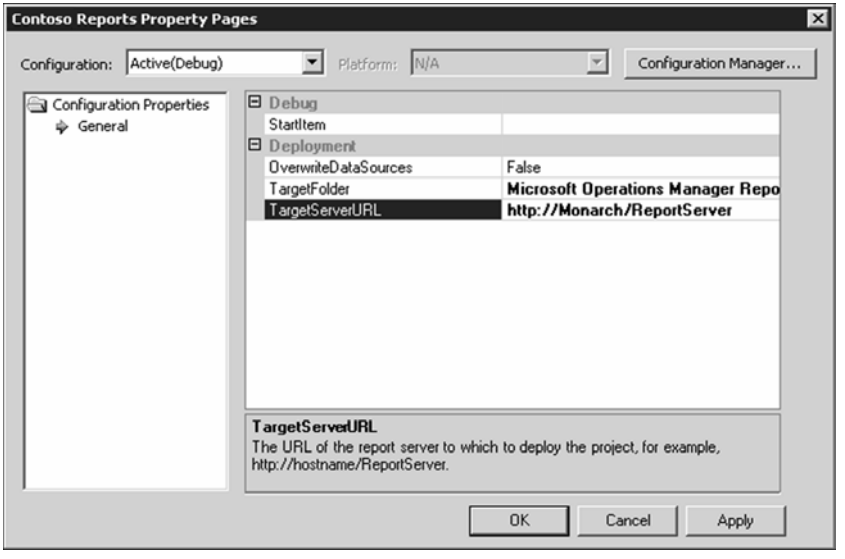


FIGURE 21.24 Reports Property Pages window.

4. From within the Solution Explorer right-click on one of the reports and select Deploy. Visual Studio .NET 2003 will publish the report to the MOM Reporting Server. Make sure that you also publish any graphics that are part of the project and included in the report, such as the company logo used in the second report.
5. In the MOM Reporting console, a new folder called Contoso Reports will contain your newly created reports.

Don't Forget to Test!

It is a good idea to run the report and also test all other types of transactions such as subscribing to the report and exporting to the different formats to ensure the report functions correctly.

Updating the Data Source

After the report is uploaded to the reporting server you must revise the data source the report is associated with. When you upload the report to the reporting server the data

source that is part of the project is uploaded to the same folder; this data source is probably not configured with the correct settings required to run and subscribe to the report. You can either correct the data source configuration or simply point the report at the already-configured data source located under the home folder. For simplicity the preferred method is to change the data source, unless you have a business reason to maintain different data sources. Follow these steps to change the data source:

1. Navigate to the location of the report; in this case the report is located in the Contoso Reports folder.
2. Open the report. When the report opens select the Properties tab.
3. Select the Data Sources menu link located on the left side of the page.
4. Click the Browse button; browse and select the SCDW data source located in the root of the reporting server under the home folder.

Specifying the MOM Reporting Path

By default, the Microsoft Operations Manager Reporting path is not added. We suggest that you include this in the path to the deployment folder for two primary reasons:

- The primary reason to add the path is the SCDW data source we created. If you use the default path for the deployment folder you will overwrite the SCDW data source used by all reports within your reporting environment.
- If you take the default folder location without specifying the Microsoft Operations Manager Reporting in front of it, the reports will be on a peer level with the Microsoft Operations Manager Reporting folder, which makes the location of your reports unintuitive.

Microsoft has a different view on this; its recommendation is to create a folder named Custom Reports on a peer level to the Microsoft Operations Manager Reporting folder. This is documented in the MOM Management Pack Development Guide (http://go.microsoft.com/fwlink/?linkid=50020). If you create reports in the MOM Reporting folder, it is possible that future management pack updates could replace your report with a Microsoft-written report having the same name. Because SSRS does not include versioning functionality, a report with the same name would override the existing report. Be sure to keep the source to any reports you load into MOM Reporting (which you should do in any case).

5. Click OK to return to the Data Sources page; click the Apply button located near the bottom of the page to save the changes.

The advantage to keeping reports under the same data source is that all reports and subscriptions for a single data source can be easily viewed and modified by opening the data source and viewing the Reports and Subscriptions tabs. Additionally the authentication credentials and configuration can be updated easily from a central point.

Exporting Reports Using the Command Line

You can export reports on the reporting server with the RptUtil.exe utility. This utility is located on computers where the MOM client consoles are installed and on the MOM Reporting server. Follow these steps:

1. Open the Command Prompt and navigate to the location of the RptUtil.exe utility. This utility is located within the MOM client interface installation directory and the MOM reporting server installation directory.
2. Run the RptUtil.exe with the appropriate switches necessary to complete the export process. Details on RPTUTIL, including the minimum list of command-line switches necessary to export the report template, are provided in Chapter 12. Enter the command in the following format.

   ```
   RptUtil.exe /option1:value1 /option2:value2
   ```

Gotcha When Exporting Reports

If you need to export your reports to XML do *not* export just the specific report that you are interested in. If you export only the report, the SCDW does not work, and as a result the exported report will have an invalid data source. Export the full directory of the reports instead.

3. If the MOM reporting server is not using Secure Sockets Layer (SSL), you will be warned about the insecure connection. Press Enter to continue with the export process. A success message is written to the screen after the report process has completed successfully.

Administration

The Reporting Server operating system (OS) and application components are similar to other systems on your network as they need regular maintenance. This includes operating system and application service packs, security patches, disk/file optimization, and regular backups. We will focus primarily on additional administration techniques and tips to help ensure the successful operation of the environment that can be done in addition to the "normal" maintenance listed previously.

Reporting Database Data Retention

The default setting for data retention is 13 months or 395 days. To view the number of days the data will be retained, you can run the following command in the SQL Query Analyzer (or SQL Management Studio):

```
SELECT cs.cs_TableName 'Table Name', wcs.wcs_GroomDays 'Groom Days'
From WarehouseClassSchema wcs Join ClassSchemas cs
On cs.cs_ClassID = wcs.wcs_ClassID
```

```
Where
cs.cs_TableName = 'SC_AlertFact_Table' and
wcs.wcs_MustBeGroomed = 1 or
cs.cs_TableName = 'SC_AlertHistoryFact_Table' and
wcs.wcs_MustBeGroomed = 1 or
cs.cs_TableName = 'SC_AlertToEventFact_Table' and
wcs.wcs_MustBeGroomed = 1 or
cs.cs_TableName = 'SC_EventFact_Table' and
wcs.wcs_MustBeGroomed = 1 or
cs.cs_TableName = 'SC_EventParameterFact_Table' and
wcs.wcs_MustBeGroomed = 1 or
cs.cs_TableName = 'SC_SampledNumericDataFact_Table' and
wcs.wcs_MustBeGroomed = 1
```

To change the number of days the data will be retained, you can run the following SQL commands. The following statements configure the database to store information for 90 days. The value representing the number of days is highlighted; depending on your requirements you can change the value to retain the data for a longer or shorter period of time.

```
exec p_updategroomdays 'SC_AlertFact_Table', 90
exec p_updategroomdays 'SC_AlertHistoryFact_Table', 90
exec p_updategroomdays 'SC_AlertToEventFact_Table', 90
exec p_updategroomdays 'SC_EventFact_Table', 90
exec p_updategroomdays 'SC_EventParameterFact_Table', 90
exec p_updategroomdays 'SC_SampledNumericDataFact_Table', 90
```

If you are using SQL Server 2000, you can run the SQL Query Analyzer with one of the previously listed queries:

1. Open the SQL Query Analyzer on the reporting server. The program is located under Start, All Programs, Microsoft SQL Server, Query Analyzer.
2. In the Connect to SQL Server window, type the name of the SQL Server in the field provided and select Connect Using Windows Authentication. Click OK.
3. Select Query, Change Databases from the menu. Select the SystemCenterReporting database from the list. Click OK.
4. In the Details window type one of the queries used to set or check the data retention time of the reporting database.
5. Select Query, Execute from the menu to run the query.
6. The query is executed against the SystemCenterReporting database, and the result is displayed in a window just below the code.

Queries in a SQL Server 2005 Environment

SQL Server 2005 uses the SQL Server Management Studio; the SQL Query Analyzer is no longer available. Perform the following steps to run a query using the Management Studio:

1. Open the Management Studio on the reporting server. The program is located under Start, All Programs, Microsoft SQL: Server 2005, SQL Server Management Studio.
2. In the Connect to Server window, type the name of the SQL Server in the Server Name field, select Windows Authentication, and click Connect.
3. Under the Databases folder in the Object Explorer node (on the left side of the Management Studio), right-click on the SystemCenterReporting database and select New Query.
4. Use the Query window to type one of the queries used to set or check the data retention time of the reporting database.
5. Above and just to the left of the Query window press the ! Execute button to run the query.
6. The query is executed against the SystemCenterReporting database, and the result is displayed in a window just below the code.

Customizing the DTS Job

The DTS job only copies new data to the reporting database. This new data must have been committed to the database for at least 5 minutes before it is transferred by the DTS job. This 5 minute latency is done to ensure data consistency and can be controlled by passing a latency switch to the DTS executable.

Operations Data Grooming

By default the operations database is set to groom data older than four days. The operations database will actually store data for 60 days as a safeguard to prevent data loss in the event the DTS job does not run and the operations data is not transferred to the reporting database.

If the DTS job has not run for several days a large amount of data can build up in the operations database. For the DTS job to work successfully, the reporting database transaction log file needs to be large enough to accommodate five times the amount of data that needs to be transferred. This means that if you collect 2GB of data per day and have five days' worth of data to be transferred to the reporting database, the reporting database transaction log file needs to accommodate as much as 50GB of data for the DTS job to properly work. By using the latency switch you can transfer the data from the operations database one day at a time. For example if you have five days' worth of data in the operations database, the following switch can be added to the DTS job to prevent all data from being transferred that has not been committed to the database for more than four days:

```
/latency:4
```

After the data from the fifth day has been successfully transferred you can set the latency to three days, then two days, and so on until all the data has been transferred. The latency switch can then be removed from the DTS job to revert to the default of 5 minutes.

Configuring Security

A granular approach can be taken to securing MOM Reporting due to its tight integration with Active Directory. By defining groups within Active Directory and assigning the groups roles on the reporting server, an administrator can utilize normal Active Directory user management to provide a seamless experience for anyone needing access to reports using the Reporting console. Our discussion of security on the reporting server is divided into the following three sections, and the options can be accessed by clicking on the Site Settings site-wide menu item:

- Site-wide security
- Item-level roles
- System-level roles

Site-Wide Security and System-Level Roles

The Site-wide security and System-level roles area is used to define and grant role-based access to site-related functionality. The administrator of the reporting server can use the site-wide security settings to change the access level of a role, create a new site-wide role, and delegate administrative functions to other users or administrators. The following security settings are available when creating new or modifying existing site-wide roles:

- Manage jobs
- Mange report server properties
- Manage report server security
- Manage roles
- Manage shared schedules
- View report server properties
- View shared schedules

By default, only the System Administrator and System User site roles exist when the reporting server is deployed. The local Administrators group on the reporting server is automatically added to the System Administrator role when the reporting server is installed, meaning that anyone added to that group on the reporting server, such as the Domain Admins group, is automatically granted full access to the Reporting console. The reporting administrator can easily manage roles by adding a Windows security group or user account to one of the existing roles or a newly defined role.

Item-Level Roles

The item-level roles area is used to define role-based access to all items within the reporting server. These items can be folders, reports, data sources, or any other type of object that exists when browsing the content of the reporting site. Four roles are created by default when the reporting server is installed. These roles are given a specific set of security rights that define their functionality. A System Administrator can use the item-level roles area to create new roles with custom access permissions or change the security rights associated with existing roles. It is a good practice to leave the default roles alone and create new roles with custom security rights if the built-in roles are not adequate for your environment.

When browsing the contents of the reporting server an administrator can use the item-level roles defined in this area by selecting the Security menu found within the Properties tab of any item. From the Item Security page, specific access can be granted to a Windows user account or security group using the defined roles. The following procedure demonstrates how to grant a security group Browser role access to the Home folder of the reporting server. The Browser role is commonly used for "general" user access to the reporting server. Perform the following steps:

1. Navigate to the Home folder by clicking on the Home menu item.
2. Select the Properties tab.
3. Click the New Role Assignment button.
4. In the field provided enter the group in the Domain\Group Name format.
5. Check the Browser role from the list of available roles.
6. Click OK to save the changes.

The group specified in step 4 has now been granted Browser rights to all items in the reporting server with the exception of any objects explicitly configured to not inherit security rights from its parent. By default the Browser role has the following abilities:

- Manage individual subscriptions
- View folders
- View reports
- View resources

All objects inherit permissions from their parent by default. When viewing the Security page of an item you will notice that the New Role Assignment button is replaced with the Edit Item Security button. You can click the Edit Item Security button to override the inherited security settings.

Reverting Back to Inherited Security

When the Edit Item Security button is clicked a notification message is displayed stating that the inherited properties from the parent item will be overridden if you continue. Don't worry, if you continue you can always change the security back to default by clicking the Revert to Parent Security button that is displayed after you break the security inheritance.

Changing Email Settings

After the Simple Mail Transfer Protocol (SMTP) installation in the SQL Reporting Server is complete, the only way to change the SMTP server and email address is by editing the RSReportServer.config file in *%ProgramFiles%*\Microsoft SQLServer\MSSQL\Reporting Services\ReportServer. The relevant portion of the file is displayed in the following code with the SMTPserver and From address setting highlighted:

```
<Extension Name="Report Server Email"
Type="Microsoft.ReportingServices.EmailDeliveryProvider.EmailProvider,
ReportingServicesEmailDeliveryProvider">
<MaxRetries>3</MaxRetries>
<SecondsBeforeRetry>900</SecondsBeforeRetry>
<Configuration>
     <RSEmailDPConfiguration>
     <SMTPServer>mail.contoso.com</SMTPServer>
     <SMTPServerPort></SMTPServerPort>
     <SMTPAccountName></SMTPAccountName>
     <SMTPConnectionTimeout></SMTPConnectionTimeout>
     <SMTPServerPickupDirectory></SMTPServerPickupDirectory>
     <SMTPUseSSL></SMTPUseSSL>
     <SendUsing></SendUsing>
     <SMTPAuthenticate></SMTPAuthenticate>
     <From>MOMReporting@contoso.com</From>
     <EmbeddedRenderFormats>
          <RenderingExtension>MHTML</RenderingExtension>
     </EmbeddedRenderFormats>
     <PrivilegedUserRenderFormats></PrivilegedUserRenderFormats>
     <ExcludedRenderFormats>
          <RenderingExtension>HTMLOWC</RenderingExtension>
          <RenderingExtension>NULL</RenderingExtension>
     </ExcludedRenderFormats>
     <SendEmailToUserAlias>True</SendEmailToUserAlias>
     <DefaultHostName></DefaultHostName>
     <PermittedHosts></PermittedHosts>
</RSEmailDPConfiguration>
</Configuration>
</Extension>
```

After changing the SMTP server name, save the file and restart the ReportServer service to apply the changes. You can also change who the email comes from and the SMTP SSL and SMTP authentication settings within this file.

Changing SSL Settings

Using SSL is recommended for securing reporting server communication. If the SSL option was not selected during the SQL Server Reporting Services installation, you must manually edit two configuration files on the reporting server and install a certificate on the web server to enable SSL communication.

1. The first step is to edit the RSReportServer.config file located in the *%ProgramFiles%*\Microsoft SQLServer\MSSQL\Reporting Services\ReportServer folder on the reporting server. The relevant portion of the file follows; the settings that need to be changed are highlighted.

```
<InstanceId>MSSQL.1</InstanceId>
<InstallationID>{6ef1f7f5-27a5-4896-af5e-f11d58183e3e}</InstallationID>
<Add Key="SecureConnectionLevel" Value="3"/>
<Add Key="InstanceName" Value="MSSQLSERVER"/>
<Add Key="ProcessRecycleOptions" Value="0"/>
<Add Key="CleanupCycleMinutes" Value="10"/>
<Add Key="SQLCommandTimeoutSeconds" Value="60"/>
<Add Key="MaxActiveReqForOneUser" Value="20"/>
<Add Key="DatabaseQueryTimeout" Value="120"/>
<Add Key="RunningRequestsScavengerCycle" Value="60"/>
<Add Key="RunningRequestsDbCycle" Value="60"/>
<Add Key="RunningRequestsAge" Value="30"/>
<Add Key="MaxScheduleWait" Value="5"/>
<Add Key="DisplayErrorLink" Value="true"/>
<Service>
     <IsSchedulingService>True</IsSchedulingService>
     <IsNotificationService>True</IsNotificationService>
     <IsEventService>True</IsEventService>
     <PollingInterval>10</PollingInterval>
     <MemoryLimit>60</MemoryLimit>
     <RecycleTime>720</RecycleTime>
     <MaximumMemoryLimit>80</MaximumMemoryLimit>
     <MaxAppDomainUnloadTime>30</MaxAppDomainUnloadTime>
     <MaxQueueThreads>0</MaxQueueThreads>
     <UrlRoot>https://server01/ReportServer</UrlRoot>
     <UnattendedExecutionAccount>
          <UserName></UserName>
          <Password></Password>
          <Domain></Domain>
     </UnattendedExecutionAccount>
     <PolicyLevel>rssrvpolicy.config</PolicyLevel>
</Service>
```

2. Next, edit the RSWebApplication.config file located in the *%ProgramFiles%*\Microsoft SQL Server\MSSQL\Reporting Services\ReportManager directory on the reporting server. The relevant portion of the file follows; the settings that need to be changed are shown below:

```
<UI>
     <ReportServerUrl>https://server01/ReportServer</ReportServerUrl>
</UI>
```

3. Finally, install a certificate from a public or private certificate authority on the reporting services web server. The common name of the certificate needs to match the name of the server listed in the configuration files.

4. After installing the certificate on the web server and making the changes to both files, restart the ReportServer service to apply the changes.

Notice that the SecureConnectionLevel setting has four available values, each providing a different level of security. Table 21.1 describes each of these security levels. We recommend using Level 3 because it provides the most security by forcing all transactions to use SSL. During the SQL Server Reporting Services installation you can enable the SSL check box, but you cannot explicitly set the security level in the RSReportServer.config file. If the IIS server hosting the reporting services site is configured to require a secure channel (SSL), the security level in the RSReportServer.config file is automatically set to Level 3. However, if the site does not force the use of SSL, the security setting in the RSReportServer.config file is set to Level 2.

Changing SSL Requirements

If the SSL requirement on the website is changed, the security level in the RSReportServer.config file should also be updated.

TABLE 21.1 SecureConnectionLevel Settings

Security Level	Functionality	IIS Configuration
3	The reporting server uses SSL for all transactions.	A certificate is required, and the option to Require a Secure Channel (SSL) should be enabled.
2	The reporting server uses SSL for all potentially sensitive transactions including rendering reports.	A certificate is required, but the option to Require a Secure Channel (SSL) can be disabled.
1	The reporting server allows HTTP but prevents some transactions that could send clear-text credentials over the network.	Certificate is not required, but some actions are not allowed unless a certificate is installed, such as adding/changing data sources.
0	Reporting server does not require SSL for any transactions.	Certificate is not required.

Archiving and Changing the Data Source

You can keep the reporting database from becoming too large by archiving the data to another server. This is useful if you intend to keep the data past the default 395 day retention period or just want to maintain a smaller database size. The following procedure outlines the steps required to set up an additional data source so that you can continue to run reports against the archived reporting database:

1. Restore the database to a new location. This can be performed by simply backing up the current reporting database and then restoring through the SQL Enterprise Manager, SQL Management Studio, or any compatible third-party backup application.
2. Configure the permissions on the archive reporting database. Using the SQL Enterprise Manager (or Management Studio), grant access to the archive database by adding a Windows user account to the Security \ Logins folder. The default database should be set to the archived reporting database; the permissions for the archive database should be set to allow "public" and "SC DW Reader" access. If desired you can use the same service account the MOM reporting database is configured with.
3. Create a new data source through the MOM Reporting console. The New Data Source button is located on the toolbar under the Contents tab of the report server. For simplicity the new data source should be created in the root of the reporting server alongside the primary data source; to get to the root of the reporting server click on the Home site-wide menu item.
4. Enter the Name of the data source. The name of the data source can be anything but should reflect its general purpose—for example, **Archived Data 2005**.
5. Enter the data source Connection Type. The data source connection type should be set to Microsoft SQL Server unless you've archived the data to a different type of database that requires a custom connection.
6. Enter the Connection String. Enter the connection string in the following format:

   ```
   data source=<server name>;initial catalog=<archive database>
   ```

   For example to connect to a database called ARCHIVE2005 on a server called Ridgeway enter the following connection string:

   ```
   data source=Ridgeway;initial catalog=ARCHIVE2005
   ```

7. Set the data source connection options. Select the radio button Credentials Stored Securely in the report server. In the User name and Password fields set the credentials of the user who was granted SC DW Reader and Public access in step 2. Check the Use as Windows Credentials When Connected to the Data Source option.
8. Save the new data source. Click OK at the bottom of the page to save the new data source.

After the archived report database is created and the data source established, configure some reports to use the new data source. For simplicity you should make a copy of any existing reports and store them in a new folder that lets the report viewer know that the data is being accessed from an archive database. The following steps can be used to configure a report to use the new data source:

1. Open the report you want to change.
2. After the report opens, select the Properties tab.
3. Select the Data Sources menu link to open the Data Sources Configuration page.
4. Click the Browse button on the Data Sources page. Select the newly created data source—for example, the new data source will be called Archive Data 2005, and it should be located under the Home folder. Click OK to save the selection and return to the Data Sources Properties page.
5. Scroll to the bottom of the page and click Apply to save the changes.

You may want to take the original SystemCenterReporting database and then test reports to the archive database to ensure successful communication.

Summary

Trend analysis of business systems is often considered a necessity in many organizations that understand the need to drive efficiency, lower IT costs, and see real-world functional benefits of management systems. MOM 2005 Reporting is a powerful aspect of the MOM 2005 product that delivers this level of functionality for an array of potential audiences that includes anyone studying trends, analyzing patterns, or making infrastructure-based decisions. In this chapter several topics were covered, including

- The different components that work together to define MOM 2005 Reporting, along with the functionality associated with each of these components
- Day-to-day tasks such as site navigation through the MOM Reporting console, along with the most common features and activities such as running reports and creating scheduled report delivery
- Creating and modifying reports, along with administration tips to help maintain and secure the reporting server site

Without question the report development process is the most complex aspect of MOM Reporting. It is important to remember that we only scratched the surface of the capabilities available when designing reports. We highly encourage you to continue exploring the vast possibilities available with this product to understand the true capabilities and value of MOM Reporting.

This page intentionally left blank

CHAPTER 22

Using and Developing Scripts

IN THIS CHAPTER

Microsoft Operations Manager (MOM) 2005 offers excellent functionality for monitoring and responding to conditions on managed systems. Rules in management packs perform specific actions when predefined conditions occur. These actions can include sending a notification if a particular event is generated or changing the State view of a monitored service. The most common actions are accessible through the Administrator console without needing any customized development, are simple to implement, and can accommodate a reasonable number of common scenarios.

When the built-in elements of a rule do not meet the objectives required to monitor your environment, you can extend MOM's functionality with scripts and managed code assemblies. By developing and implementing custom scripts and managed code assemblies to respond to particular criteria, you can achieve a much greater level of control and cover an almost limitless number of scenarios.

Response Elements Within MOM Rules

Rules in MOM are made up of several different configurable elements. A rule's response can be configured to perform a number of different actions, based on the type of rule implemented. The following list shows common responses that can be triggered within most types of rules:

- Running a script
- Sending an SNMP trap
- Sending a notification

- Executing a command or batch file
- Updating a state variable
- Transferring a file
- Calling a method on a managed code assembly

This chapter focuses on gaining a better understanding of how to implement and test script and managed code responses within MOM 2005. We will demonstrate the setup and configuration of rules that utilize the "Launch a Script" and "Call a Method on Managed Code Assembly" responses. We will also discuss designing scripts that interact with MOM by utilizing the ScriptContext Application Programming Interface (API) and Managed Code Runtime API.

Security

The MOM Host process executes both script and managed code responses. Several different instances of the MOM Host process can run simultaneously on a managed system. This is by design; each instance is responsible for a different type of response such as executing a script, executing managed code, running a batch file, or collecting performance data. Each instance of this process is executed under the context of the Action account, and responses initiated by the MOM Host process also run under the context of the Action account.

For the most part, the MOM Host process runs outside the MOM Service process with the exception of specific threads. Separating the MOM Host and MOM Service processes provides performance enhancements and helps ensure that potential problems with a response will not necessarily impede the functionality of other MOM agent components or communication with the management server.

ScriptContext API

MOM can be configured to Launch a Script as a response in a custom rule. When a script is executed on a target system, the ScriptContext object is automatically made available within the script runtime. This object allows the script to interact with the various MOM elements.

For example, a script that verifies specific settings can be executed on a target system through a MOM rule. This script can use the ScriptContext object to generate and send events with specific severity levels based on results of the verification. When developing custom scripts, the ScriptContext object is considered the starting point to access other objects in the MOM scripting library. We discuss the ScriptContext object along with other objects in the MOM scripting library in the next sections of this chapter.

When developing scripts for MOM, you can theoretically use any ActiveX scripting language as long as the engine needed to execute the script is installed on the target system. Microsoft provides engines for two scripting languages with the Windows platform, allowing you to natively run scripts written in the VBScript and JScript languages.

This chapter provides examples written in VBScript. We used VBScript because most scripts included with existing Microsoft management packs are written with VBScript, and it is a simple language to learn and understand when you're getting started with scripting.

Managed Code Runtime API

Managed code responses can be executed on target systems by configuring a rule to Call a Method on a managed code assembly. Assemblies are stored outside the MOM database and are not automatically installed on the target system. When the assemblies are built you must manually or programmatically add the assembly to the systems that will execute the response. Managed code assemblies can be used to interact with the operating system or application being monitored and can also be designed to interact with the various MOM elements.

When developing managed code responses, you can use any of the .NET programming languages included with the Visual Studio .NET suite. The examples in this chapter are written in Visual Basic .NET because it closely resembles VBScript and is easy to learn.

Both Within a Rule

Each of the following rules can be configured to initiate a script or call a method on a managed code assembly in response to conditions in a rule matching predefined criteria:

- Event rules—alert on or respond to event
- Event rules—detect missing events
- Alert rules
- Performance rules

Event rules can also be configured to run responses at a predefined time or on a specific interval, which is often used to discover characteristics or run an analysis on the target system.

Use the Administrator console to configure a rule to run a response. To configure one of the previously listed rules with a custom response, follow these steps:

1. Open the MOM 2005 Administrator console.
2. Go to Management Packs \ Rule Groups, and navigate to the rule you want to configure.
3. Right-click on the rule and select Properties.
4. When the Properties window opens, select the Responses tab.

Figure 22.1 shows the Responses tab of an event rule. This rule is configured to execute a response script called MOM Agent Service Discovery on a predefined interval. Several configuration options are required when adding either a script or a managed code

response to a rule to ensure that the response runs correctly. The following two procedures demonstrate how to customize the response elements of rules:

- Configuring a script response—This procedure will configure the response element of a rule to launch a custom script.
- Configuring a managed code response—This procedure will configure the response element of a rule to call a method on a managed code assembly.

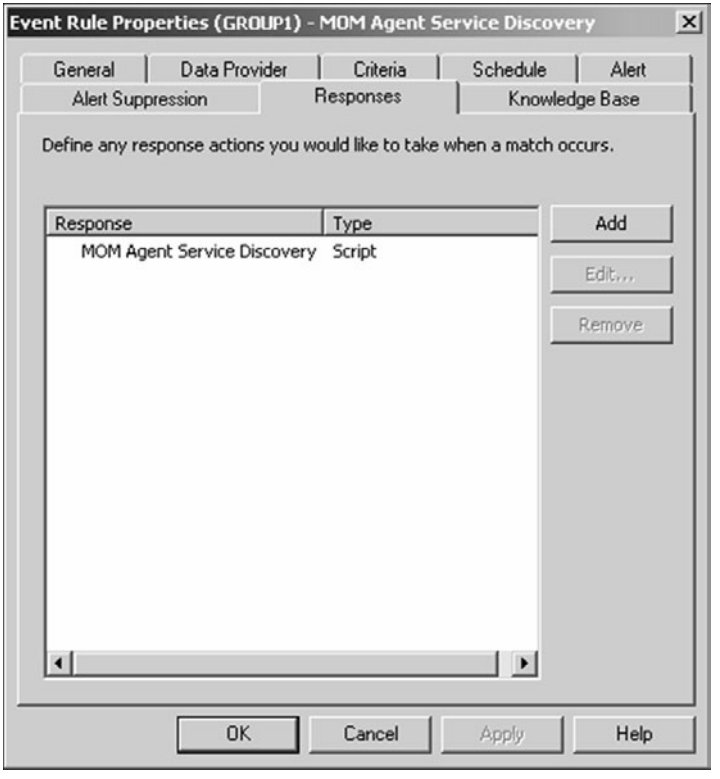


FIGURE 22.1 Event Rule Responses tab.

Configuring a Script Response

The following steps configure a MOM rule to launch a script response:

1. Open the MOM Administrator console.
2. Go to Management Packs \ Rule Groups, and navigate to the rule you want to configure.

3. Right-click on the rule and select Properties.
4. When the Properties window opens, select the Responses tab.
5. Click the Add button.
6. Select Launch a Script from the drop-down menu.

In the Launch a Script window you can select an existing script from the drop-down menu or create a new script to use as the response. The following procedure can be used to create a new script:

1. Select the New button to open the Script Properties Window.
2. Enter the Name of the script.
3. Enter a Description for the script.
4. Select the script Language from the drop-down menu.

Using "Custom" Script Languages

If your script is not written in VBScript or JScript you must select Custom from the Language drop-down menu. The custom script (such as PerlScript) must identify the script engine on the first line of code to work correctly.

Microsoft provides references to both VBScript and JScript at its MSDN scripting website, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnanchor/html/Scriptinga.asp.

5. Click the Next button to show the source code window.
6. Copy and paste or type your script code in the window.
7. Click Next to show the Parameters window.

At this point you can configure your script to accept parameters; skip this step if your script does not take parameters. To add parameters to your script, follow these steps:

1. Click the Add button to open the Script Parameters window.
2. Enter the Name of the parameter.
3. Enter the Value of the parameter.
4. Enter the parameter Description.
5. Click OK to return to the Parameters window.

   Repeat these steps as necessary for each parameter you are adding to the script.
6. Click Finish to return to the Launch a Script window.

Using Script Parameters

For the parameters to work correctly the script must use the ScriptContext.Parameters property to retrieve the value of each parameter. The "Creating a New Script" section later in the chapter demonstrates how to use this property to retrieve the configured parameters.

Figure 22.2 shows an example of the Launch a Script screen after each of the options is configured. After configuring the properties of the script, click OK to return to the Responses tab of the rule. After a rule is configured to launch a script response, you can edit or remove the script by selecting the Edit or Remove buttons on the Responses tab within the rule.

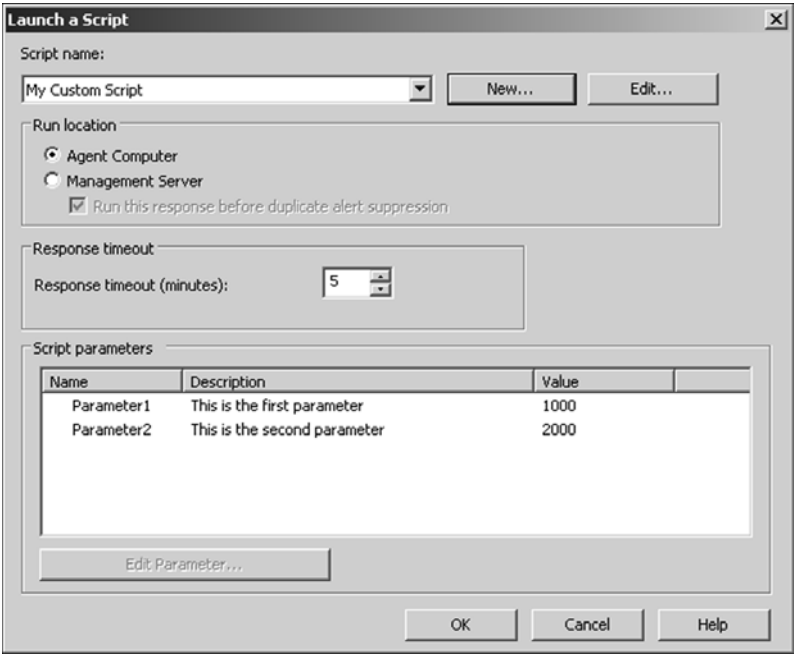


FIGURE 22.2 Launch a Script screen.

The Launch a Script screen allows you to configure the following script-related properties:

- Run Location—This configures where the script is executed from. The run location can be set to Agent Computer or Management Server and be configured to run before duplicate alert suppression is invoked.
- Response Timeout—This setting configures how many minutes the script can run before it is stopped by MOM. When debugging scripts you should increase the default value to prevent the debug session from ending prematurely. The settings can be configured from 1 to 60 minutes, with 5 minutes being the default.

- Script Parameters—These parameters are optional and required only if the script is designed to accept them.

When the script is added to the rule it is stored in the Operations database and distributed to all agent-managed systems that the rule applies to. By navigating to the Management Packs \ Scripts folder, you can view all available scripts in the database. You can use this folder to add scripts to or remove scripts from the database.

If you add a script directly to the Scripts folder you can set the default values for the various parameters accepted by the script. When you add a script as a response to a rule the parameters have these default values, although you can specify a different set of values for them. New parameters specified in a rule do not affect the original parameters associated with the script.

Configuring a Managed Code Response

The following procedure demonstrates how to configure a MOM rule to call a method on a managed code assembly:

1. Open the MOM Administrator console.
2. Go to Management Packs \ Rule Groups and navigate to the rule you want to configure.
3. Right-click on the rule and select Properties.
4. When the Properties window opens, select the Responses tab.
5. Click the Add button.
6. Select Call a Method on a Managed Code Assembly.

Several configurable options are available from the Configure a .NET Framework Response window:

- Run location—The run location specifies where the managed code assembly is executed from. The setting can be from the agent-managed computer or the management server and can be configured to run before duplicate alert suppression is invoked.
- Response Timeout—This setting configures how many minutes the assembly can run before it is stopped. When debugging managed code you should increase the default value to prevent the debug session from ending prematurely. The settings can be configured from 1 to 60 minutes. The default is 5 minutes.
- Assembly Name—When specifying the Assembly Name you need to include the name of the assembly, the version, culture, and public key. This information can be obtained with the Managed Code Response Utility, which is discussed in the "Creating and Configuring a Managed Code Response" section later in this chapter.
- Fully Qualified Type Name—The fully qualified name is specified as Namespace.Class. This information can be obtained with the Managed Code Response Utility.
- Method Name—This is the name of the method on the assembly you want to use. This information is available from the Managed Code Response Utility.

- Method Type—This option allows you to configure the type of method being used in the assembly.
- Method Parameters—The parameters for the assembly are optional and are required only if the assembly is designed to accept them. The managed code assembly must be configured to accept an instance of the MOM runtime context for it to work with MOM data types.

The following steps demonstrate how to add method parameters to your managed code response from within the Configure a .NET Framework Response window.

1. Select the Add button.
2. Select the Type from the drop-down menu.
3. Enter the Value for the type in the field provided.
4. Click OK to add the parameter.

You can repeat these steps to add additional parameters. Remember that parameters are passed to the method in the order they appear. Use the buttons found on the left side of the parameters list to move the parameters up or down, edit existing parameters, or remove them from the list. Figure 22.3 shows an example of a fully configured managed code assembly response.

The MOM runtime context does not require a value. This parameter must be added to allow your managed code to interact with the various MOM elements. If your assembly does not need to interact with MOM, passing this parameter is not required.

When configuring method parameters, be aware of Microsoft knowledge base article 885725, which describes a bug requiring you to enter the property ID instead of the name of the parameter. You can view this article at http://support.microsoft.com/kb/885725/.

External to MOM

The following items are external to MOM and not covered in this chapter:

- When a response rule is created several options can be selected, including the ability to send a notification to a notification group, transfer a file, and so on. Only Running a Script and Calling a Method in a Managed Code Assembly are covered in this chapter because they relate directly to extending MOM's functionality with scripts and managed code responses.
- SQL views are commonly used when developing custom reports to perform trend analysis. The SQL views can also be used by your custom script or managed code to access data found within the Operations database and the Reporting database.
- The MOM WMI providers and the MOM Helper Objects have both been depreciated and should not be used when developing new response scripts. This applies only to the MOM WMI providers, not WMI calls in general. Microsoft's future direction is to access MOM through .NET because this gives increased efficiency when working with large amounts of data. When developing response scripts you can use the ScriptContext object and built-in operating system APIs to achieve the same functionality as available in these depreciated items.

- The Microsoft.EnterpriseManagement.Mom (Microsoft.Mom.Sdk.dll) and Microsoft.EnterpriseManagement.Mom.Runtime (MOM.Context.dll) namespaces are defined in the MOM Management Server Class Library (MCL) These namespaces are used to develop managed code that can interact with the different MOM elements. The Microsoft.EnterpriseManagement.Mom.Runtime namespace is the focus of this chapter because it is primarily used when developing managed code assemblies to be used as custom responses. The Microsoft.EnterpriseManagement.Mom namespace is commonly used when developing external applications that will interface with MOM and is not covered in this chapter. To include these assemblies in the .NET project, add a reference to the Microsoft.Mom.Sdk.dll and the MOM.Context.dll files. These files are located in the *%ProgramFiles%*\Microsoft Operations Manager 2005\SDK Bin\ folder of management servers or systems where the user consoles are installed.
- The MOM Connector Framework (MCF) provides additional namespaces for the MOM Management Server Class Library. These namespaces allow development of connectors that interface and synchronize data between MOM and external third-party applications. Microsoft's MOM-to-MOM Product Connector (MMPC) is built using the MCF. The process of developing software to use the MCF is beyond the scope of this chapter.

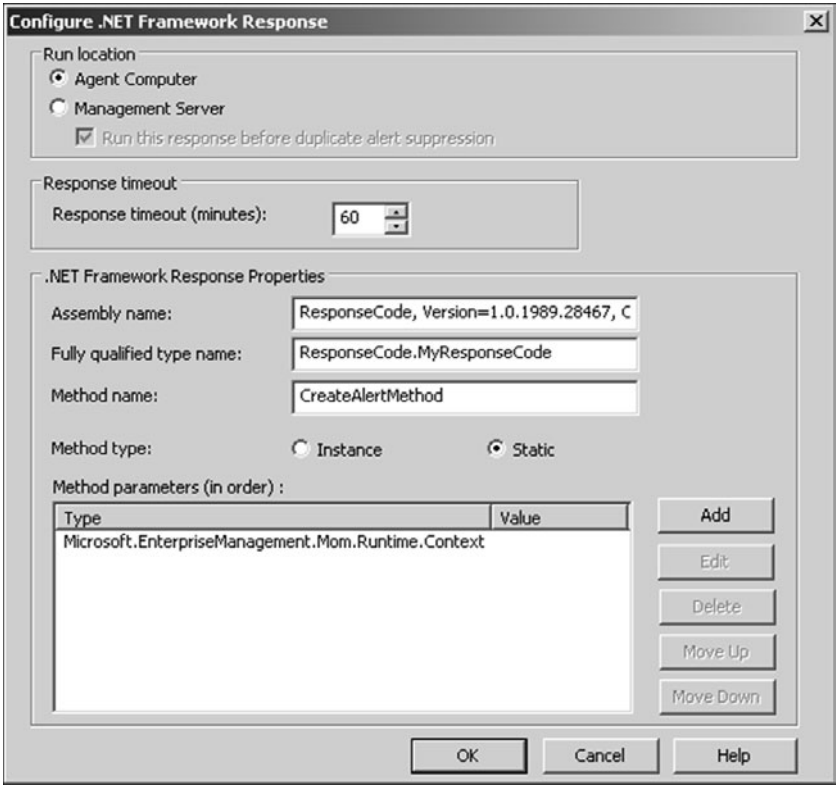


FIGURE 22.3 .NET Framework Response configuration.

ScriptContext API

The ScriptContext object is automatically initiated and available to scripts running within the MOM scripting environment. This means that you don't need to create an instance of the ScriptContext object because your custom script can immediately start using the methods and properties of this object.

ScriptContext Object

The `ScriptContext` object is available only to scripts run within the MOM scripting environment; using the MOM scripting library outside the MOM environment is not currently supported.

When developing scripts that interact with MOM, you will always start with the ScriptContext object. The object is the starting point for working with MOM data because it allows you to access the other objects found in the MOM scripting library. For example, if you want to create a new alert within your script you would use the CreateAlert method of the ScriptContext object to establish a new instance of an Alert object. After the instance of the alert is created, you can customize the alert through the methods and properties associated with the Alert object. The same procedure also exists for the other MOM-related elements, such as Events and Performance data, simply by calling the CreateEvent and CreatePerfData methods within the ScriptContext object. The following example demonstrates using the ScriptContext.CreateAlert() method to create an instance of the Alert object.

```
sub main()

    dim NewMomAlert
    set NewMomAlert = ScriptContext.CreateAlert()
    NewMomAlert.Description = "Something bad happened"

end sub
```

The main Subroutine

The subroutine `main` is executed automatically when the script is initiated on the target system.

Within the main subroutine a variable is defined named NewMomAlert. The variable is assigned a new instance of the Alert object created with the ScriptContext.CreateAlert() method. The Description property of the Alert object is then used to set the description of the newly created alert.

Scripting Library Runtime Objects

The MOM scripting library is comprised of the following runtime objects. The response script can interact with the different elements found within MOM by leveraging the methods and properties associated with each of these objects:

- Alert object
- DiscoveryData object
- DiscoveryRelationshipCollection object
- DiscoveryClassInstanceID object
- DiscoveryInstance object
- DiscoveryRelationshipInstance object
- Event object
- PerfData object
- ScriptContext object
- ScriptState object
- VarSet object

ScriptContext Object Methods and Class Properties

With the exception of the ScriptContext object, an instance of each object must be created before its associated methods and properties can be accessed. Table 22.1 describes the methods available in the ScriptContext object. These methods can be used for a number of different actions, including creating new instances of Alert, Discovery, Event, and Performance objects.

TABLE 22.1 ScriptContext Object Methods

Method Name	Returns	Description
ScriptContext.CreateAlert()	Object	Creates a new instance of the Alert object. When a new object is created it is initially empty; you can use the properties and methods associated with the Alert object to configure the new alert.
ScriptContext.CreateDiscoveryData()	Object	Creates a new instance of the DiscoveryData object. When a new object is created it is initially empty; you can use the properties and methods associated with the DiscoveryData object to configure the new alert.

TABLE 22.1 Continued

Method Name	Returns	Description
`ScriptContext.CreateEvent()`	Object	Creates a new instance of the Event object. When a new object is created it is initially empty. You can use the properties and methods associated with the Event object to configure the new alert.
ScriptContext.CreatePerfData()	Object	Creates a new instance of the Performance Data object. When a new object is created it is initially empty; you can use the properties and methods associated with the PerfData object to configure the new alert.
ScriptContext.GetScriptState()	Object	Used to get or create new script state variables, the script state variables are maintained until the MOM service is cycled.
ScriptContext.IsAlert()	Boolean	This method can be used to determine whether an alert initiated the script. You should use this method before attempting to access the properties associated with the Alert object.
ScriptContext.IsEvent()	Boolean	This method can be used to determine whether an event initiated the script. You should use this method before attempting to access the properties associated with the Event object.
ScriptContext.IsPerfData()	Boolean	This method can be used to determine whether performance data initiated the script. You should use this method before attempting to access the properties associated with the PerfData object.
ScriptContext.GetOverride(*override name*)	String	This method is used to get the specified override.
ScriptContext.Echo(*variable name or text*)	String	This method is used to write information to the trace log file on the target system. Logging must be enabled in the registry of the target system for this method to work correctly.

TABLE 22.1 Continued

Method Name	Returns	Description
ScriptContext.Sleep(*number of seconds*)	Long	This method can be used to suspend the execution of the script for a specific period of time.
ScriptContext.Quit()	—	This method can be used to exit the script at a specific point.
ScriptContext.Submit(*object name*)	—	After a new Alert, Discovery, Event, or Performance object is created and configured, this method is used to send the information to the management server.

Table 22.2 describes the properties available in the ScriptContext object. These properties are used to retrieve information about the target system along with the rule that triggered the script. These properties can also be used to retrieve details of the Alert, Event, and Performance objects that caused the script to execute on the target system.

TABLE 22.2 ScriptContext Class Properties

Property Name	Returns	Description
ScriptContext.Alert	Object	This property allows you to get the Alert object that initiated the script. Use the methods and properties associated with the Alert object to retrieve the Alert details.
ScriptContext.Event	Object	This property allows you to get the Event object that initiated the script. Use the methods and properties associated with the Event object to retrieve the Event details.
ScriptContext.PerfData	Object	This property allows you to get the Performance Data object that initiated the script. Use the methods and properties associated with the PerfData object to retrieve the PerfData details.
ScriptContext.ProcessingRule	Object	This property allows you to get the rule object that initiated the script. Use the properties associated with the Rule object to retrieve the Rule details.
ScriptContext.Parameters	Object	This property retrieves the script parameters as specified in the MOM Administrator console.

TABLE 22.2 Continued

Property Name	Returns	Description
ScriptContext.IsTargetAgentless	Boolean	This property can be used to determine whether the target system has a MOM agent installed.
ScriptContext.IsTargetVirtualServer	Boolean	This property can be used to determine whether the target system is a virtual node of a cluster.
ScriptContext.ManagementGroupName	String	Returns the name of the management group.
ScriptContext.Name	String	Returns the name of the script.
ScriptContext.TargetComputer	String	Returns the name of the target system.
ScriptContext.TargetComputerIdentity	String	Returns the domain and name of the target system.
ScriptContext.TargetNetBIOSComputer	String	Returns the NetBIOS name of the target system.
ScriptContext.TargetNetBIOSDomain	String	Returns the NetBIOS domain name of the target system.
ScriptContext.TargetFQDNComputer	String	Returns the FQDN of the target system.

For examples demonstrating how to use many of these methods and properties, see the "Creating a New Script" section later in this chapter.

Managed Code Runtime API

The Microsoft.EnterpriseManagement.Mom.Runtime namespace is a part of the MOM Management Server Class library. Similar in nature to the ScriptContext object used for developing script responses, managed code assemblies use the Context class in this namespace as a starting point to interact with other classes. The following is an example of an empty class that can be used to start your managed code assembly in Visual Basic .NET 2003:

```
Imports Microsoft.EnterpriseManagement.Mom

Public Class MyResponseCode

    Public Shared Sub CreateAlertMethod(ByVal context As _
      Microsoft.EnterpriseManagement.Mom.Runtime.Context)

    End Sub

End Class
```

This code defines a single method called CreateAlertMethod and accepts the Microsoft.EnterpriseManagement.Mom.Runtime.Context as a parameter. When configuring the MOM rule to execute the method, you only need to pass the Context class as a method parameter if your assembly will interact with MOM. For example, if you want your assembly to create an alert or get a state variable value you must pass the Context class to the assembly. If you didn't develop the managed code assembly you can still use it to perform actions on the operating system or application you are monitoring, you just won't be able to pass the Context class required for MOM interaction. If you have assemblies used to manage third-party applications, you may want to develop a wrapper that takes the Context class, allowing you to send alerts and such back to the management server.

Managed Code Responses

As a prerequisite, MOM requires the .NET Framework 1.1 to be installed on the system where the assembly will be executed. The assembly file should also be copied to the same folder as the MOMHost.exe file or preferably to the global assembly cache. To interact with the various MOM data types, your assembly needs to reference the MOM.Context.dll file because this file defines the Microsoft.EnterpriseManagement.Mom.Runtime namespace. The managed code must also be configured to accept the Microsoft.EnterpriseManagement.Mom.Runtime.Context as a parameter. For detailed information on all namespaces found with the MOM Management Server Class Library, review the Microsoft Operations Manager 2005 SDK at http://go.microsoft.com/fwlink/?linkid=50272.

Managed Code Runtime Namespace

The Microsoft.EnterpriseManagement.Mom.Runtime namespace is used primarily when developing managed code responses. The following classes are available within this namespace. Review the Microsoft Operations Manager 2005 SDK for a detailed listing of all the methods and properties for each class within this namespace.

- Context
- ResponseTarget
- RuntimeAlert
- RuntimeEvent
- RuntimePerformanceData
- State
- VariableSet

Analyzing Existing Scripts

Many of the existing Microsoft management packs come with scripts that perform a variety of actions. It is useful to understand how these scripts work if you want to modify or tune them for your own environment. This section is divided into the following two procedures that analyze some of the scripts within the MOM 2005 management pack:

- MOM Test End to End Monitoring—This looks at the basic functionality found within the MOM Test End to End Monitoring script. This script is simple in nature; it performs a single operation against the target system. The script is initiated by the Test End to End Monitoring task found in the Tasks pane of the Operator console.

Operator Tasks

Tasks available through the Operator console can also be used to execute a custom script or call a method on a managed code assembly.

- MOM Action Account Password Expiration Check—This script looks into the structure of a more complex script. The script accepts parameters that are defined in the Administrator console, calls different operating system and Active Directory objects, and sends alerts back to the management server if a problem is detected or threshold is exceeded.

All scripts are contained within the OnePoint database and can be viewed in a single location within the Administrator console. To locate and view the entire repository of available MOM scripts, perform the following steps:

1. Open the MOM 2005 Administrator console.
2. Navigate to Management Packs \ Scripts.

The Detail pane now displays all the scripts that have been either manually created or imported with existing management packs. From within the Scripts folder you can add new scripts or remove existing scripts from the MOM database.

MOM Test End to End Monitoring

This first script demonstrates some of the more basic MOM scripting functionality. The MOM Test End to End Monitoring script creates an event on the target system with a specific event number. Creating the event triggers the MOM End to End Monitoring rule, which generates a Success alert.

Code Differences

Some of the code in this chapter may be wrapped or shortened for readability; refer to the original code within the script for the complete syntax.

The End to End Monitoring script is written in VBScript and is initiated through a task in the Operator console. To begin, open the properties of the script:

1. Open Management Packs \ Scripts within the MOM Administrator console.
2. Select the MOM Test End to End Monitoring script.
3. Right-click and select Properties.
4. The Properties window will open; select the Script tab.

The script code can be modified directly within the Script tab. It is helpful when looking at a script to copy the contents from the default MOM script editing window to a text or script editor that can be expanded to the entire screen size.

1. The first statement after the comments specifies that each variable must be declared or the script will not run. This is a handy technique to avoid spelling mistakes.

```
Option Explicit
```

2. The second part of this script defines five constants; each constant is given a value representing the type of event being created. For example, if a warning event is created the EventType property of the Event object is assigned the EVENT_TYPE_WARNING constant, which translates to the value of 2. The MOM Operator console then displays this event as a yellow triangle with the exclamation point.

```
Const EVENT_TYPE_SUCCESS = 0
Const EVENT_TYPE_ERROR = 1
Const EVENT_TYPE_WARNING = 2
Const EVENT_TYPE_INFORMATION = 4
Const EVENT_TYPE_AUDITSUCCESS = 8
Const EVENT_TYPE_AUDITFAILURE = 16
```

3. The next part of the script creates the new event. In the first line we declare the variable oEvent. The following line stores an instance of the Event object in the oEvent variable by calling the CreateEvent method of the ScriptContext object.

```
Dim oEvent
Set oEvent = ScriptContext.CreateEvent()
```

4. The oEvent variable now contains a new instance of the Event object. You can use the different methods and properties available to the Event object to define the event. The EventSource property is set to "Microsoft Operations Manager", the EventNumber property is set to 1000000000, and so on.

```
With oEvent
    .EventSource = "Microsoft Operations Manager"
    .EventType = EVENT_TYPE_INFORMATION
    .EventNumber = 1000000000
```

```
    .Message = "This event is used by Microsoft" &_
     "Operations Manager to verify end to end" &_
     "monitoring is working successfully"
End With
```

Using the With Statement

The With statement allows you to access a series of properties without needing to qualify each one. The same result would be achieved by adding oEvent before each of the properties being set.

5. After the event properties are configured, the Submit method of the ScriptContext object is used to send the event to the management server. Creating this event triggers the MOM End to End Monitoring rule, generating a Success alert.

```
ScriptContext.Submit oEvent
```

As you can see, the ScriptContext object is relatively simple to use when you need to access and create different MOM data types. Each time you run the Test End to End Monitoring task in the Operator console the event is created on the target system. Understand that the event created is not listed in the event log of the target system; this event is generated and used internally by MOM. This type of event is also known as an *internal MOM event*.

MOM Action Account Password Expiration Check

This second script demonstrates some of the more advanced MOM scripting functions. The purpose of the MOM Action Account Password Expiration Check script is to determine the number of days until the Action account password expires. An Error or Critical Error is generated if the number of days exceeds any of the threshold parameters passed to the script.

The script demonstrates how to get parameters that can be configured within the Administrator console, how to access Active Directory to check the password expiration date, and how to access the operating system to determine the security context of the Action account.

The MOM Action Account Password Expiration Check script is written in VBScript and initiated through the MOM Action Account Password Expiration Check rule located under Management Packs \ Rules \ Microsoft Operations Manager \ Operations Manager 2005 \ Agents on all MOM roles \ Event Rules. By default this rule is configured to run daily at 4:00 a.m.

1. To begin, open the properties of the script by opening the Scripts folder in the Administrator console.
2. Within this folder select the MOM Action Account Password Expiration Check Script and select Action and then Properties from the menu.

3. On the Properties window select the Script tab.

4. As with most other scripts, this script starts by defining constants that can be used throughout the script. Values are defined for each of the different Alert Levels the Alert object can be configured with. The ADS_UF_DONT_EXPIRE_PASSWD constant is also defined; this constant represents the value of a password that does not expire. Not all constants are located at the top of the script. Additional constants are set throughout the script, and each constant is initialized before the script executes.

```
Option Explicit
Const ADS_UF_DONT_EXPIRE_PASSWD = &h10000
Const ALERT_SUCCESS = 10
Const ALERT_INFORMATION = 20
Const ALERT_WARNING = 30
Const ALERT_ERROR = 40
Const ALERT_CRITICAL_ERROR = 50
Const ALERT_SECURITY_BREACH = 60
Const ALERT_SERVICE_UNAVAILABLE = 70
```

5. After defining constants, define a VBScript class called Error. This class is used for error handling within the script. You can use a VBScript class as a technique to create your own object complete with methods and properties. For additional information on the Class statement, refer to a VBScript language reference (such as the one Microsoft provides at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnanchor/html/Scriptinga.asp).

```
Class Error
    Private m_lNumber
    Private m_sSource
    Private m_sDescription
    Private m_sHelpContext
    Private m_sHelpFile
    Public Sub Save()
        m_lNumber = Err.number
        m_sSource = Err.Source
        m_sDescription = Err.Description
        m_sHelpContext = Err.HelpContext
        m_sHelpFile = Err.helpfile
    End Sub
...
End Class
```

6. The first subroutine in the script is called Main, which is executed automatically when running within the MOM environment. The first two lines of the Main subroutine define variables to hold parameters passed to the script. The two lines

following the variable definition use the ScriptContext.Parameters.Get method to retrieve the parameters that were defined within the Administrator console.

```
Sub Main()
 Dim lErrorAlertThresholdDays
 Dim lCriticalErrorAlertThresholdDays
 lErrorAlertThresholdDays = CLng(ScriptContext.Parameters.Get...
 lCriticalErrorAlertThresholdDays = CLng(ScriptContext.Parameters.Get...
...
```

7. This next part of the Main subroutine calls the MomCreateObject function. This function assigns an instance of the WinNTSystemInfo object to the objNTSystemInfo variable. The WinNTSystemInfo object is not part of the MOM scripting library; it is available as part of the Windows operating system.

```
Dim objNTSystemInfo
Set objNTSystemInfo = MomCreateObject("WinNTSystemInfo")
```

8. Next, the script uses the UserName and DomainName properties of the WinNTSystemInfo object to retrieve the user name and domain name of the user running the script. The Action account is now identified.

```
Dim sDomain
On Error Resume Next
sDomain = objNTSystemInfo.DomainName
On Error Goto 0
Dim sUser
sUser = objNTSystemInfo.UserName
```

9. After retrieving the user name and domain name, the script tests the value of each. If the value of the domain is empty and the value of the user account matches "SYSTEM", then the Action account is running under the Local System context. As the password for the Local System context is controlled automatically, the script doesn't need to keep processing. The Quit method of the ScriptContext object is used to exit the script at this point.

```
If sDomain = "" And StrComp(sUser, "SYSTEM", vbTextCompare)=0 Then
    ScriptContext.Quit
End If
```

10. The script continues if the Action account is not running under the local system context. The next step retrieves the user account the Action account is using. The script uses the name and domain value retrieved in the previous step with the ADSI object, allowing you to retrieve an instance of the account from the domain. If the user cannot be found in the domain, the ThrowScriptError function is called.

```
On Error Resume Next
Set objUser = GetObject("WinNT://" & sDomain & "/" & sUser & ",user")
```

```
e.Save
On Error Goto 0
If e.Number <> 0 Then ThrowScriptError ...
```

11. If the user is found in the directory, the password expiration flag is checked and compared against the ADS_UF_DONT_EXPIRE_PASSWD constant. If the UserFlags are equal to the value of the constant, the password for the account is set to never expire and the script does not need to keep processing. The Quit method of the ScriptContext object will exit the script at this point.

```
If objUser.Get("UserFlags") And ADS_UF_DONT_EXPIRE_PASSWD Then
    ScriptContext.Quit
End If
```

12. If the Action account password is not configured to expire, the script continues. The difference between the current date and the date the password on the account is set to expire is calculated and stored in the lDaysUntilPasswordExpires variable.

```
Dim sAccount
sAccount = sDomain & "\" & sUser
Dim lDaysUntilPasswordExpires
lDaysUntilPasswordExpires = DateDiff("d", Date(), &_
    objUser.PasswordExpirationDate)
```

13. The lDaysUntilPasswordExpires variable is then compared against each parameter passed to the script. If the number of days until the password expires is less than or equal to one of the parameters, a corresponding error is created by calling the CreateAlert subroutine.

```
If lDaysUntilPasswordExpires <= lCriticalErrorAlertThresholdDays Then
    CreateAlert ...  ALERT_CRITICAL_ERROR
ElseIf lDaysUntilPasswordExpires <= lErrorAlertThresholdDays Then
    CreateAlert ...  ALERT_ERROR
End If
```

This script demonstrates some of the more advanced functions of the ScriptContext object while also showing how to access different parts of the operating system and Active Directory. We will next look at the different subroutines and functions the Main subroutine calls.

1. The CreateAlert subroutine is used to create the alert when the password expiration date for the Action account has exceeded one of the predefined thresholds. The account name, the number of days until the password expires, and the alert level are all passed to the CreateAlert subroutine:

```
Sub CreateAlert(ByVal sAccount, ByVal lDays, ByVal lAlertLevel)
...
```

2. The MomCreateObject function is used to return an instance of an object based on the name is passed to the sProgramID argument. In this script, this function is used once to create an instance of the WinNTSystemInfo object. The WinNTSystemInfo object is used to retrieve the user name and domain name of the account that is running the script, which will be the Action account.

```
Function MomCreateObject(sProgramId)
...
```

3. The ThrowScriptError and ThrowScriptErrorNoAbort functions are called when an error is encountered and the user name cannot be read from Active Directory.

```
Function ThrowScriptError(sMessage, oErr)
...
Function ThrowScriptErrorNoAbort(sMessage, oErr)
...
```

4. The following functions are not used by this script. You will notice that many of the scripts contain the same functions and basic structure. This was most likely done to speed up development time by creating reusable functions and subroutines. Unfortunately, the scripts are not very well documented and the extra code can be confusing.

```
Function IsValidObject(ByVal oObject)
Function WMIGetObject(sNamespace)
Function WMIGetInstance(sNamespace, sInstance)
Function WMIGetInstanceNoAbort(sNamespace, sInstance)
Function WMIExecQuery(sNamespace, sQuery)
Function GetWMIProperty(oWmi, sPropName, nCIMType, ErrAction)
```

Creating a New Script

This section goes through the process of creating new scripts and demonstrates how to use the different methods and properties associated with the objects in the MOM scripting library. We also show how to create and configure a simple managed code assembly. The section is divided into the following areas:

- Using the ScriptContext object—This example demonstrates how to use the methods and properties found in the ScriptContext object. The ScriptContext object allows you to retrieve information about the environment and allows you to create new instances of other objects found in the MOM scripting library.
- Using the ScriptState and VarSet objects—This example shows how the VarSet object is used to store and retrieve information each time the script runs.

- Passing variables to a script—This example demonstrates how to configure your script to accept variables and how to configure the Administrator console to pass variables to your script.
- Creating and configuring a managed code response—The example steps through the process of creating a managed code assembly and how to configure the different options required to set up your managed code response within a MOM rule.

Setting Up a Test System

Before developing script and managed code responses you should identify a development computer to use for running script and managed code responses. We do not recommend using a production system for development. The following process can be used to set up a development computer:

1. Identify a system that can be used for testing. It is highly recommended to develop script and managed code responses in a proof of concept (POC) environment and not on production systems.
2. Create a new computer group to hold your test systems. You can create a new computer group by opening the Administrator console and navigating to Management Packs \ Computer Groups. Right-click on the Computer Groups folder and select Create Computer Group to start the creation wizard. While running the Computer Group Creation Wizard, you should manually add the test computer to the group.
3. Create a new rule group to hold your test rules. You can create a new rule group by opening the Administrator console and navigating to Management Packs \ Rule Groups. Right-click on the Rule Groups folder and select Create Rule Group to begin creating the rule group. During the rule group creation, you should associate this rule group with the computer group containing your test systems.
4. Create custom rules or tasks to run your test scripts and managed code responses. You can create a rule to test your script and managed code responses. One of the easiest ways to test your responses is to create an event rule designed to Alert on or Respond to Event. Configure this rule to respond to a custom event number. You can then use the MOM 2005 Resource Kit Event Creator utility to generate the custom event in the event log of the test system to trigger the event rule. Another way to invoke your script is with a custom task in the Operator console.

Using the ScriptContext Object

This section discusses using the methods and properties found within the ScriptContext object. This object is the starting point for working with MOM data because it provides the capability to retrieve information about the environment and create instances of other objects found within the MOM scripting library.

The following example is written in VBScript and can be triggered on the target system in a variety of ways. You could execute this script through a timed event, a task, or by creating a synthetic event in the event log on the target system to trigger a custom rule. When developing a custom script it is often easier to code the script in a text or script editor rather than typing it in the script source code window within the Administrator console.

1. The first part of this script defines the constants for the AlertLevel property, the ProblemState property, and the ResolutionState property of the Alert object. These properties require the numeric value, not the name of the value.

```
option explicit

const Level_Success = 10
const Level_Information = 20
const Level_Warning = 30
const Level_Error = 40
const Level_Critical_Error = 50
const Level_Security_Issue = 60
const Level_Service_Unavailable = 70

const Problem_Investigate = 0
const Problem_Inactive = 1
const Problem_Active = 3

const Resolution_New = 0
const Resolution_Acknowledged = 85
const Resolution_Level_1 = 170
const Resolution_Level_2 = 180
const Resolution_Level_3 = 190
const Resolution_Level_4 = 200
const Resolution_Resolved = 255
```

2. The main subroutine declares a variable called oCustomAlert; an instance of a new Alert object is assigned to the oCustomAlert variable. This is accomplished by calling the CreateAlert method of the ScriptContext object.

```
sub main()
  dim oCustomAlert
  set oCustomAlert = ScriptContext.CreateAlert()
```

3. After a new instance of the alert is created, the properties of the Alert object can now be used to configure the alert. The properties of the Alert object can be configured simply by assigning a value to the various properties. The TargetNetbiosComputer property and the TargetNetbiosDomain property of the ScriptContext object are used to assign the name and domain of the computer running the script to the corresponding properties of the new alert.

```
    with oCustomAlert
      .AlertLevel = Level_Success
      .AlertSource = ScriptContext.TargetNetbiosComputer
      .Computer = ScriptContext.TargetNetbiosComputer
      .ComputerDomain = ScriptContext.TargetNetbiosDomain
      .Description = "This is a test alert"
      .Name = "Test Alert"
      .ProblemState = Problem_Investigate
      .ResolutionState = Resolution_New
    end with
```


4. Finally, the new alert is sent to the management server by passing the oCustomAlert object to the Submit method of the ScriptContext object.

```
    ScriptContext.Submit(oCustomAlert)
end sub
```

The previous script demonstrates how to use the ScriptContext object to create a Success alert and send it to the management server. The final code should look similar to the following:

```
option explicit

const Level_Success = 10
const Level_Information = 20
const Level_Warning = 30
const Level_Error = 40
const Level_Critical_Error = 50
const Level_Security_Issue = 60
const Level_Service_Unavailable = 70

const Problem_Investigate = 0
const Problem_Inactive = 1
const Problem_Active = 3

const Resolution_New = 0
const Resolution_Acknowledged = 85
const Resolution_Level_1 = 170
const Resolution_Level_2 = 180
const Resolution_Level_3 = 190
const Resolution_Level_4 = 200
const Resolution_Resolved = 255

sub main()
  dim oCustomAlert
  set oCustomAlert = ScriptContext.CreateAlert()
```

```
  with oCustomAlert
    .AlertLevel = Level_Success
    .AlertSource = ScriptContext.TargetNetbiosComputer
    .Computer = ScriptContext.TargetNetbiosComputer
    .ComputerDomain = ScriptContext.TargetNetbiosDomain
    .Description = "This is a test alert"
    .Name = "Test Alert"
    .ProblemState = Problem_Investigate
    .ResolutionState = Resolution_New
  end with

  ScriptContext.Submit(oCustomAlert)
end sub
```

You can change this Success alert to a Critical Error alert by simply assigning a different number or constant to the AlertLevel property of the Alert object. For example, if you assign the AlertLevel property the value of 50 or the Level_Critical_Error constant, the critical error icon is displayed in the Operator console rather than the success icon.

The alert can be changed in other ways by changing values associated with the corresponding property. At the end of this chapter we list each of the properties available for the Alert object and other objects available in the MOM scripting library.

Reading and Writing Properties

When creating a new alert, almost every property can be assigned a value. This is not the case when you get the properties of the alert that triggered the script. The properties of the alert triggering the script are read-only and cannot be changed, with the exception of the AlertHistory property.

This characteristic applies to the other objects in the MOM scripting library such as the Event, Rules, and PerfData objects.

Using the ScriptState and VarSet Objects

This section demonstrates how to use the ScriptState and VarSet objects found within the MOM scripting library. The ScriptState and VarSet objects can store variables that can be accessed the next time the script runs.

The ScriptState method of the ScriptContext object retrieves and updates values of variables stored by the VarSet object. The following example is written in VBScript:

1. The first part of this script defines the constants for the VarSet name and VarSet instance used by the script. The VarSet is automatically created if it does not exist.

```
option explicit
const VarSet_Name = "Error Counter"
const VarSet_Error_Count = "Number of Errors"
```

2. The main subroutine of the script configures the variables that will hold an instance of each object.

```
sub main()
  dim oVarSet
  dim oWarningVarSet
  dim iErrorCount
```

3. The oVarSet variable is assigned an instance of the ScriptState object by calling the GetScriptState method of the ScriptContext object. The oWarningVarSet variable is then assigned an instance of the "Error Counter" VarSet object by calling the GetSet method of the VarSet object. If the "Error Counter" VarSet does not exist the object is created automatically.

```
  set oVarSet = ScriptContext.GetScriptState()
  set oWarningVarSet = oVarSet.GetSet(VarSet_Name)
```

4. The iErrorCount variable is assigned the value of the "Number of Errors" VarSet instance. The VarSet instance is created if it does not exist. The iErrorCount is then incremented by 1.

```
  iErrorCount = oWarningVarSet.get(VarSet_Error_Count)
  iErrorCount = CLng(iErrorCount) + 1
```

5. Next the Put method of the VarSet object is called. The Put method accepts the VarSet instance name and the new value that will be assigned to the instance. The SaveSet method of the ScriptState object is then called to save the changes.

```
  call oWarningVarSet.put(VarSet_Error_Count, iErrorCount)
  call oVarSet.SaveSet(VarSet_Name, oWarningVarSet)
```

6. This last line writes the value of the VarSet instance to the trace log file:

```
  ScriptContext.Echo iErrorCount
end sub
```

The VarSet and ScriptState objects are useful when you need to store and retrieve a value each time a script runs on the target system. The VarSet object remains on the system until the MOM service is restarted and can be accessed by any of the scripts executing on the target. The object is stored locally on the target system. You can also use a variable stored centrally on the management server by using the State object. Storing the variable centrally on the management servers allows any script on any system to access the value. For additional information about the State object see the MOM SDK documentation. The complete code should look similar to the following:

```
option explicit
const VarSet_Name = "Error Counter"
const VarSet_Error_Count = "Number of Errors"
```

```
sub main()
  dim oVarSet
  dim oWarningVarSet
  dim iErrorCount

  set oVarSet = ScriptContext.GetScriptState()
  set oWarningVarSet = oVarSet.GetSet(VarSet_Name)

  iErrorCount = oWarningVarSet.get(VarSet_Error_Count)
  iErrorCount = CLng(iErrorCount) + 1

  call oWarningVarSet.put(VarSet_Error_Count, iErrorCount)
  call oVarSet.SaveSet(VarSet_Name, oWarningVarSet)

  ScriptContext.Echo iErrorCount
end sub
```

Passing Parameters to a Script

The next example demonstrates how to pass parameters defined in the Administrator console to variables defined in the script. The script portion of this example is written in VBScript. To start, a new script configured to accept parameters will be assigned as a response within a MOM rule:

1. Open the MOM Administrator console.
2. Navigate to Management Packs \ Rule Groups.
3. Navigate to the rule you want to configure.
4. Right-click on the rule and select Properties.
5. When the Properties window opens, select the Responses tab.
6. Click the Add button.
7. Select Launch a Script from the drop-down menu.

The Launch a Script window opens, allowing you to create a new script that accepts parameters. Follow these steps:

1. Select the New button to open the Script Properties.
2. Enter **My Custom Script** in the Name field.
3. Select VBScript in the Language drop-down menu.
4. Click Next to show the source code window.

5. Type the following code in the script code window:

```
option explicit
sub main()
  dim sParm1
  dim sParm2
  sParm1 = ScriptContext.Parameters.Get("FirstParameter")
  sParm2 = ScriptContext.Parameters.Get("SecondParameter")
  ScriptContext.Echo "Parameter 1: " & sParm1
  ScriptContext.Echo "Parameter 2: " & sParm2
end sub
```

6. Click Next to show the Parameters window.

This script is configured to accept two parameters called "FirstParameter" and "SecondParameter". Use the following steps to add the corresponding parameters to the Script Properties - Parameters window:

1. Select the Add button to open the Script Parameters window.
2. Type **FirstParameter** in the Name field.
3. Enter **6** in the Value field.
4. Click OK to return to the Parameters window.
5. Select the Add button.
6. Type **SecondParameter** in the Name field.
7. Enter **840000** in the Value field.
8. Click OK to return to the Parameters window.
9. Click Finish to return to the Launch a Script window.

Parameter Names

The name of the parameter you configured in the Administrator console must match the name of the parameter passed to the Get method within the script.

In this particular case, the Get method looks for two parameters called "FirstParameter" and "SecondParameter". Figure 22.4 shows how the Launch a Script will look after being configured in the previous steps. Click OK to close the window and return to the rule Properties window.

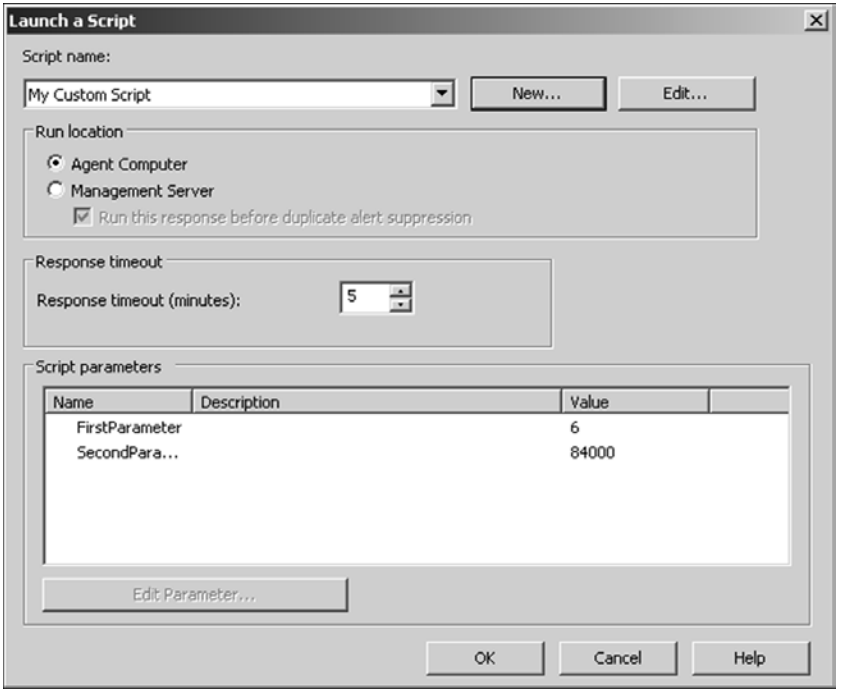


FIGURE 22.4 Launch a Script window.

The rule is now configured to pass the value of FirstParameter and SecondParameter to the script when it is executed on the target system. The script in this example uses the Get method to retrieve the value of each parameter and assign it to the corresponding sParm1 and sParm2 variable.

Creating and Configuring a Managed Code Response

In this section we demonstrate how to create a managed code assembly, install the managed code assembly on the system that will be executing the response, and finally how to configure the rule with the correct settings to successfully execute the method in the assembly.

MOM requires that all managed code assemblies be signed. You can use the Microsoft .NET Framework Strong Name Utility to create the key pair that will be used to sign your assembly. This utility is called SN.EXE and is located in the *%ProgramFiles%*\Microsoft Visual Studio .NET 2003\SDK\v1.1\Bin folder of a system where Visual Studio .NET is installed. The following steps use the SN.EXE utility to create the key pair file on your development system:

1. Select Start, Run and type **CMD**; click OK.
2. Navigate to the folder with the SN.EXE utility.
3. Type **SN.EXE -k c:\mykey.snk**.

The file mykey.snk will be created in the root of the C: drive; the name and location can be changed to something more appropriate. The next step in the process is establishing a new project within Visual Studio .NET 2003:

1. Open Visual Studio .NET 2003.
2. Select the File, New, Project from the menu.
3. Select Visual Basic Projects from the Types list.
4. Select Class Library from the Templates list.
5. Enter a Name for the project; click OK.

A new project will be created and the Class1.vb file is opened. Next you will tell your project to use the key pair file you created. To reference the key pair file, do the following:

1. Select View, Solution Explorer from the menu.
2. Navigate to the Solution Explorer pane.
3. Double-click the AssemblyInfo.vb file to display the file contents.
4. Type the following code at the bottom of the file:

```
<Assembly: AssemblyKeyFile("C:\mykey.snk")>
```

The AssemblyInfo.vb file should look similar to the following; note that the comments have been removed for readability. The mykey.snk line has been highlighted in bold:

```
Imports System
Imports System.Reflection
Imports System.Runtime.InteropServices

<Assembly: AssemblyTitle("")>
<Assembly: AssemblyDescription("")>
<Assembly: AssemblyCompany("")>
<Assembly: AssemblyProduct("")>
<Assembly: AssemblyCopyright("")>
<Assembly: AssemblyTrademark("")>
<Assembly: CLSCompliant(True)>

<Assembly: Guid("DD4B9042-2A98-4A36-85D5-3BE39B2A1A8A")>

<Assembly: AssemblyVersion("1.0.*")>
<Assembly: AssemblyKeyFile("C:\mykey.snk")>
```

Next we add a reference to the MOM.Context.dll file. This file allows your assembly to interact with the MOM server and use the MOM functionality found in the MOM runtime namespace. The MOM.Contxt.dll is located in the *%ProgramFiles%*\Microsoft Operations Manager 2005\SDK Bin folder on a system with the user consoles installed.

Copy this file to the system you are developing your managed code assembly from, and add the MOM.Context.dll reference to your project:

1. Select Project, Add Reference from the menu.
2. The Add Reference window will open; click Browse.
3. Browse to the location of the MOM.Context.dll file.
4. Select the file and click the Open button.
5. Click OK to close the Add Reference window.

Now you can enter your code in the Class1.vb file. This code represents the "action" that is executed on the target system by the response rule. To enter your code, follow these steps:

1. Navigate to the Solution Explorer pane.
2. Double-click the Class1.vb file to display the file contents.
3. Replace all existing code that is already in the file with the following:

```
Imports Microsoft.EnterpriseManagement.Mom

Public Class MyResponseCode

  Public Shared Sub CreateAlertMethod(ByVal context As _
    Microsoft.EnterpriseManagement.Mom.Runtime.Context)

    Dim MyAlert As CustomAlert = New CustomAlert

    MyAlert.Name = "Managed Code Alert"

    MyAlert.Source = "Managed Code Class"

    MyAlert.ResolutionState = AlertResolutionState.[New]

    MyAlert.Severity = AlertSeverity.Error

    Context.Submit(MyAlert)

    End Sub

End Class
```

The previous code example defines a method called CreateAlertMethod. This method is configured to accept the …Mom.Runtime.Context as a parameter, allowing the assembly to create and submit the new alert to the management server.

You can now build your solution, which creates the assembly file that can be added to the global assembly cache of the server that will execute the managed code response. When you build your solution a .DLL file is created in the BIN folder located within your project folder. The BIN folder is found in the following location by default:

```
\My Documents\Visual Studio Projects\<Project Name>\Bin
```


To build your solution and add the DLL file to the global assembly cache (GAC) on the target system, perform the following steps:

1. Select Build, Solution from the menu.
2. Locate the Bin folder within your project folder.
3. Copy the DLL file to a shared network drive.
4. Log on to the system that will run the response.
5. Drag the DLL from the shared drive to the GAC.

Adding DLLs to the GAC

The path to the Global Assembly Cache is *%windir%*\assembly by default. Do not attempt to copy and paste the DLL file from the shared network location. You must drag and drop the file on the assembly folder to install the assembly correctly.

Before configuring the MOM rule to execute the managed code response you need to discover some information about your managed code. This is done with the Managed Code Response Utility. Follow these steps:

Managed Code Response Utility

The Managed Code Response Utility is found in the Microsoft Operations Manager 2005 Resource Kit. The resource kit can be downloaded from the Microsoft website and is also part of the CD content included with this book.

1. Copy the MCRUtil.exe to a folder with your DLL file.
2. Select Start, Run, type **CMD**, and click OK.
3. Navigate to the folder that contains the MCR utility and the DLL.
4. Type the following command in the CMD window:

```
mcrutil.exe responsecode.dll /method:CreateAlertMethod
```

You will need to change the name of the DLL to the actual name of your DLL file; if you changed the method name in the previous example you will also have to change the

method name on the command line. The output of the command should be similar to the following; note that the PublicKeyToken will be unique to your environment:

```
Assembly Name:
    ResponseCode, Version=1.0.1989.18465, Culture=neutral,
PublicKeyToken=324ded37eb8a65da

Fully Qualified Type Name:
    ResponseCode.MyResponseCode

    Method Name:
        CreateAlertMethod(
                Microsoft.EnterpriseManagement.Mom.Runtime.Context)
```

You can now configure a MOM rule required to execute the managed code response:

1. Open the MOM Administrator console.
2. Navigate to Management Packs \ Rule Groups and select the rule you want to configure.
3. Right-click on the rule and select Properties.
4. When the Properties window opens, select the Responses tab.
5. Click the Add button.
6. Select Call a Method on a Managed Code Assembly.

The Configure .NET framework Response window opens, allowing you to configure the details of the response. Table 22.3 lists the configuration options. Remember that the Assembly Name is unique for your environment; use mcrutil.exe to list the correct information for your file.

TABLE 22.3 ScriptContext Object Methods for Managed Code Assembly

Method Name	Description
Run Location	Agent Computer
Response Timeout	60 minutes
Assembly Name	ResponseCode, Version=1.0.1989.18465, Culture=neutral, PublicKeyToken=324ded37eb8a65da
Fully qualified type name	ResponseCode.MyResponseCode
Method name	CreateAlertMethod
Method type	Static
Method parameters	Microsoft.EnterpriseManagement.Mom.Runtime.Context

A new Error alert is sent to the management console when the managed code response is executed on the target system.

Troubleshooting Tips

This section describes the steps to troubleshoot script and managed code responses. It is highly recommended to develop and debug script and managed code responses in a POC lab and not on production systems!

Attaching the Process Debugger

If you are debugging code on a remote system, you may have problems attaching the Visual Studio .NET process debugger to the MOMHost.exe process if it runs under the Local System account. If the Action account has been configured to run as Local System, you should either debug the code with a local installation of Visual Studio .NET or change the Action account to a regular user account.

When attempting to track down and identify problems in your response code, the first step is to check the MOM Operator console for any error or warning alerts. In the case of a script response you may see an alert similar to the one shown in Figure 22.5. The alert displays useful information about the script including what type of error occurred and the line number the error occurred on. In this example a syntax error was detected, preventing script execution.

FIGURE 22.5 Script warning alert.

In the case of a managed code response, you may see an alert such as the one shown in Figure 22.6. This alert displays information about the error. The error message is not always the most meaningful although it does tell you that the code was not processed because an error occurred. In this example, analysis of the problem would reveal the public key specified in the MOM rule was incorrect.

When an error in a script or managed code response occurs in this stage of execution, no useful information is written to the trace log. Often the Visual Studio process debugger won't even "catch" the error because the response was stopped before it was executed, consequently preventing you from being able to step through the code.

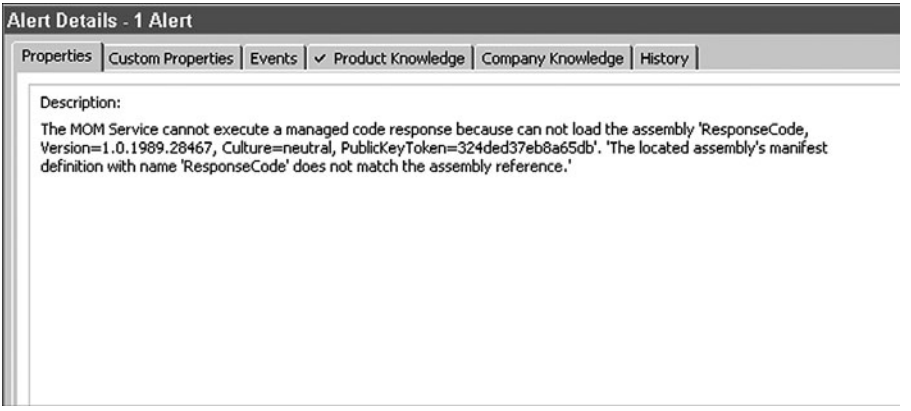


FIGURE 22.6 Managed code warning alert.

After syntax and rule configuration errors are corrected, the next step towards tracking down and identifying problems with both script and managed code responses is to enable the trace log settings in the registry. After modifying the registry, trace information for all script and managed code responses is written to the trace log file. The following information is captured in the trace log:

- Trace data captured from the response
- The name, the start time, and the end time of the response
- Information passed to the ScriptContext.Echo method within the script
- Information passed to the Context.Echo method within the managed code

Perform the following registry change to enable the trace log on the system running the response.

1. Open Regedit on the Target System. Select Start, Run; type **regedit** in the Open dialog box; and click OK. The Windows Registry Editor will open.
2. Locate the OnePoint Registry Key. The location of the OnePoint key on the target system is: HKEY_LOCAL_MACHINE\SOFTWARE\Mission Critical Software\OnePoint.
3. Set the Name of the Script you want to debug. Within the OnePoint registry key create a new STRING called DebugEnabledScript. Set the value of DebugEnabled Script to the name of the script you want to debug, or set the value to * to debug all scripts.
4. Enable Script Debugging. Within the OnePoint registry key add a new DWORD called EnableActiveDebugging. Set the value to **1** to enable script debugging.

To complete the changes restart the MOM service on the target system.

Disable Active Script Debugging

When debugging has been completed the value of the EnableActiveDebugging key should be set to 0 to disable the trace log on the next restart of the MOM service. The trace log inhibits response performance, so it should not be enabled full time.

Trace information is written to the *%windir%*\Temp\Microsoft Operations Manager folder on the target system. The name of the log file will vary depending on the run location of the response. When the response is run on a MOM agent the AgentResponses-<*management group name*>.log file is created. Running the response on a management server creates the ServerResponses-<*management group name*>.log file.

View Trace Logs in Real-time

If you open the trace log in Notepad, you must close and then reopen the log to see new entries. Alternatively, you can use the SMS Trace utility to view changes to the log file in real-time. This log viewer is available in the SMS 2003 Tool Kit v2, available for download at http://download.microsoft.com; search for "SMS Toolkit 2."

The response trace log is useful for determining when the response was executed and data has been passed to the Echo method. The primary drawback to the trace log file is that only a small amount of information is written to the log, and this data is only is only written after the response successfully executes. If the response crashes or just doesn't work correctly, the trace log may not provide enough information to troubleshoot the issue. To overcome this limitation you can attach the Visual Studio .NET process debugger to the MOMhost.exe process running the response.

The script or managed code response can be analyzed with a local or remote installation of Visual Studio .NET. To debug a process on a remote system, the remote debugging components of Visual Studio .NET must be installed on the system running the response. If the system running the response already has the full version of Visual Studio .NET installed you do not need to install the remote debugging components because they are included with the typical installation of the Visual Studio suite. To install the Visual Studio .NET remote debugging components on the remote system, do the following:

1. Start the Visual Studio .NET 2003 setup program.
2. Select Remote Components Setup from the bottom of the setup window.
3. Read through the requirements of the remote debugging components.
4. Install any necessary prerequisites.
5. Click the Install Full button to start the installation process.

After the remote debugging components are installed and debugging is enabled, you can attach the Visual Studio .NET 2003 debugger to the MOMHost.exe process. While you are debugging, your script and managed code responses are paused while you step through

the code. This may cause the response to exceed the timeout threshold configured within the MOM rule, consequently ending the response and the debugging session. By default this timeout value is set to 5 minutes. You can view the properties of the script or managed code response and modify the timeout value to between 1 to 60 minutes. The next sections go into detail on how to locate and attach the Visual Studio process debugger to the correct service.

Debugging Scripts

Several instances of the MOMhost.exe process can be running on the target system. Perform these steps to locate and attach to the MOM Host process responsible for running response scripts:

1. Open Visual Studio .NET 2003.
2. Select Tools, Debug Process from the menu.
3. In the Processes window, enable the Show System Processes check box.
4. Type the name of the remote computer in the Name field; click the Refresh button.
5. Locate each MOMHost.exe process in the available process list.
6. Select the MOMHost.exe process with Script in the Type column.
7. Select the Attach button.
8. In the Attach to Process window, enable Script, and click OK.
9. Close the Processes window by clicking Close.

The Visual Studio .NET process debugger is now attached to the MOM Host process that is responsible for executing scripts. When an error is encountered in a script, the debugger displays the script code and highlights the line causing the error. If you prefer, you can select Debug, Break All from the menu to pause the script on the first line and allow you to step through each line of code in the script.

Figure 22.7 shows an example of the Processes window. Notice that the MOMHost.exe process has Script specified in the Type column; this is the MOM Host process responsible for running response scripts.

Locating the Correct MOM Host Process

The MOM Host process loads the files required to run the script as needed. If no scripts are currently running on the target system you may not be able to locate the MOM Host process responsible for running script responses. The MOM Host process may also be cycled in specific scenarios, such as when the system receives new rules. When the MOM Host process cycles the Visual Studio .NET debugging session attached to that process also ends.

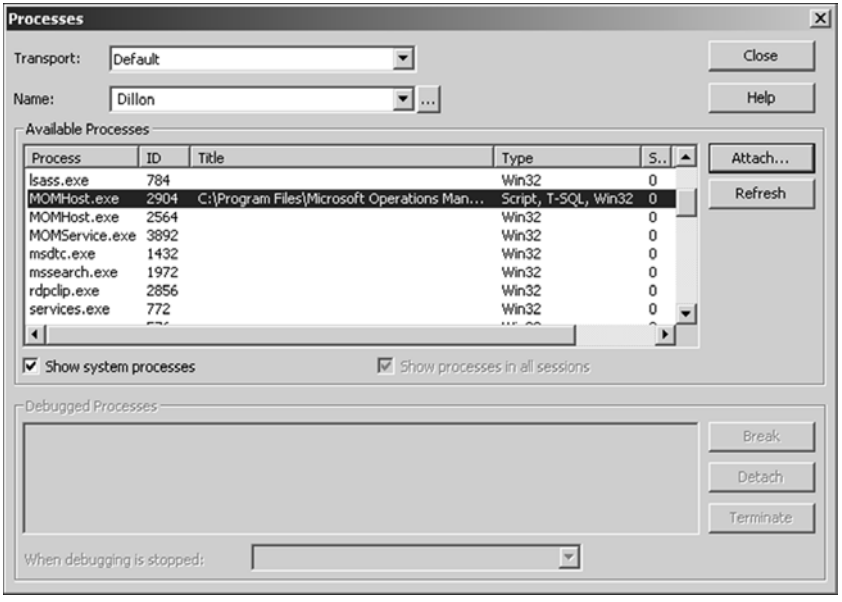


FIGURE 22.7 Processes window.

While using the Visual Studio .NET process debugger, the Debug toolbar at the top of the window (shown in Figure 22.8) allows you to move about each line of code. The tabbed windows at the bottom of the page can also assist in the troubleshooting process. For example, the Locals window, also shown in Figure 22.8, displays information such as constants, objects, and variables, and the values associated with each.

Debugging Managed Code

Debugging managed code is similar to debugging scripts, but it requires several additional steps before getting started. To prepare for the debugging process, perform the following procedure on the system running the managed code response:

1. Remove your assembly from the global assembly cache if necessary.
2. Copy the assembly DLL to the folder that holds the MOMHost.exe file.
3. Copy the assembly PDB to the folder that holds the MOMHost.exe file.
4. Restart the MOM service.

Finding the Required Files for Debugging

The managed code DLL and PDB files are normally located in the BIN folder within your Visual Studio project folder. \My Documents\Visual Studio Projects\<Project Name>\Bin is the default location for the BIN folder.

The MOMHost.exe file is located in the *%ProgramFiles%*\Microsoft Operations Manager 2005 folder by default.

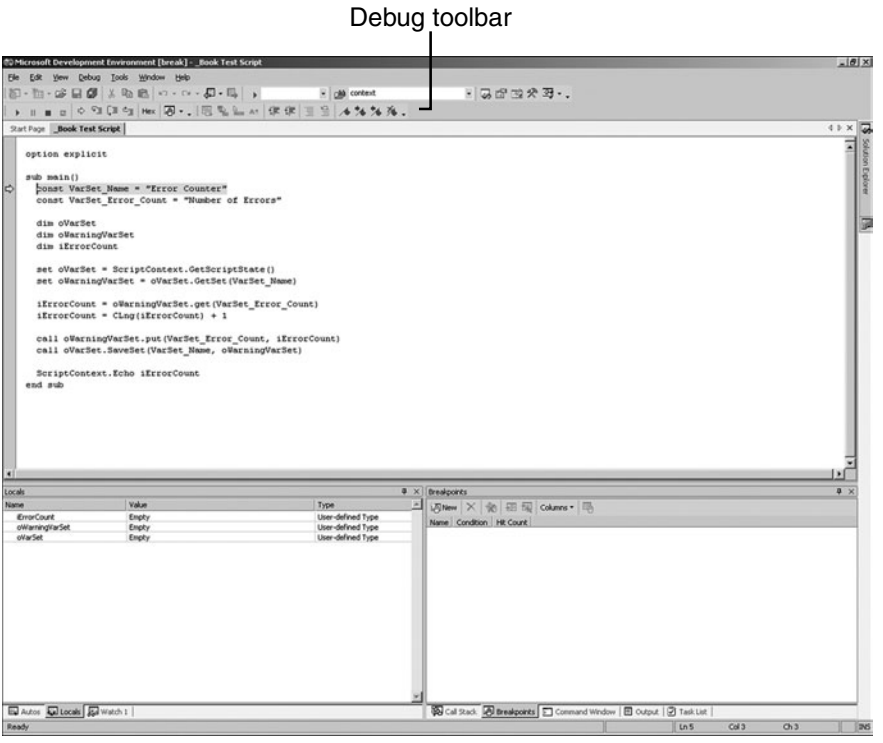


FIGURE 22.8 Debugging buttons.

Next, locate and attach the Visual Studio process debugger to the MOM Host process responsible for running the managed code response. This set of steps is done on the system you will debug your managed code from.

1. Open Visual Studio .NET 2003.
2. Open your managed code response project.
3. Select Tools, Debug Process from the menu.
4. In the Processes window, enable the Show System Processes check box.
5. Type the name of the remote computer in the Name field and click the Refresh button.
6. Locate each MOMHost.exe process in the available process list.
7. Select the MOMHost.exe process with .NET the Type column.
8. Select the Attach button.
9. Enable Common Language Runtime; click OK.
10. Close the Processes window by clicking Close.

The Visual Studio .NET process debugger is now attached to the MOM Host process responsible for executing managed code. The next step is to set a break point in your code

by right-clicking the Public Shared Sub CreateAlertMethod... line of code and selecting Insert Breakpoint from the menu. You screen should look similar to the one shown in Figure 22.9.

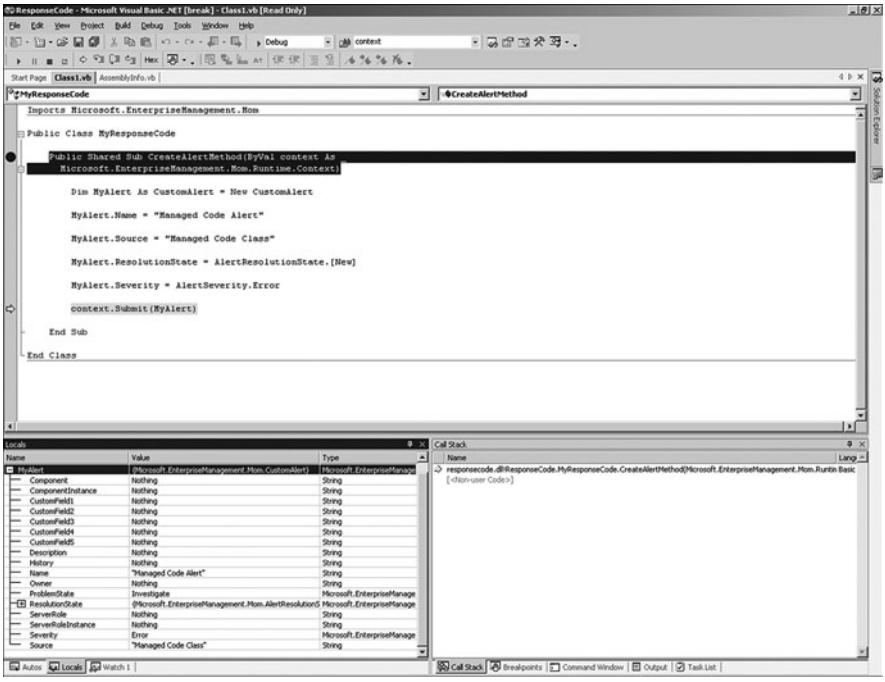


FIGURE 22.9 Managed code break point.

Now when the managed code response is triggered on the target system, the execution will pause, and you have the opportunity to step through each line of code in the assembly. While using the Visual Studio .NET process debugger, the Debug toolbar at the top of the window (shown in Figure 22.10) allows you to move about each line of code. The tabbed windows at the bottom of the page also assist in the troubleshooting process. For example, the Locals window (on the bottom half of the page), shown in Figure 22.10, displays each value contained within the MyAlert object of this assembly.

To successfully debug the managed code assembly the correct symbols must be loaded. This was accomplished in the first set of steps when the DLL and PDB files were copied to the folder containing the MOMHost.exe file. If the debugger didn't stop the code at your defined break point, verify that the symbols loaded correctly.

Select Debug, Windows, Modules from the File menu. Your managed code assembly should be listed, as shown in Figure 22.11, and the Information column should display Symbols Loaded. If the symbols that check the assembly DLL are not loaded, check whether they are being loaded from the correct location. In Figure 22.11 you can see that this assembly is correctly loaded from the *%ProgramFiles%*\Microsoft Operations Manager 2005 folder on the target system. This folder also contains the symbols file (the PDB file) associated with the managed code assembly.

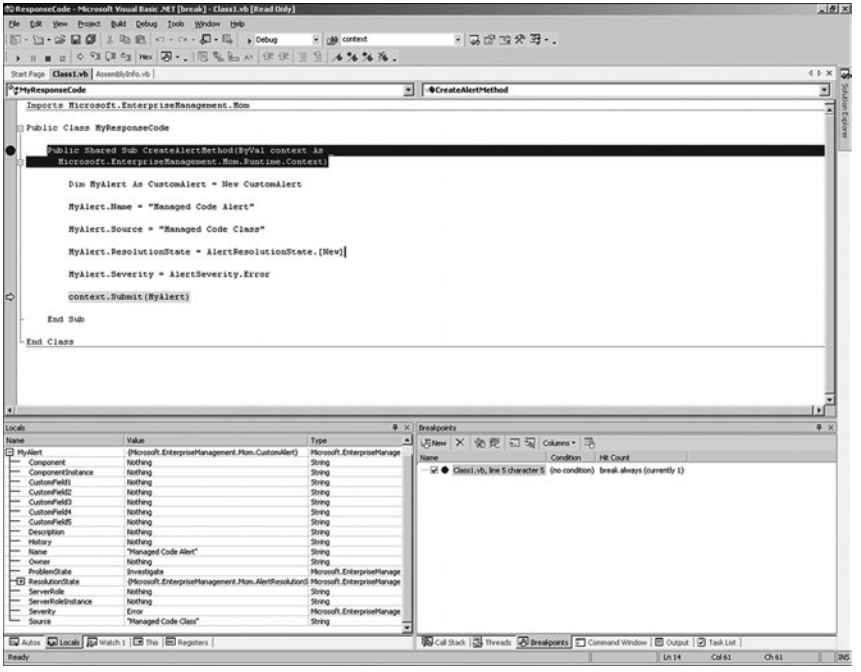


FIGURE 22.10 Managed code break point—Locals window.

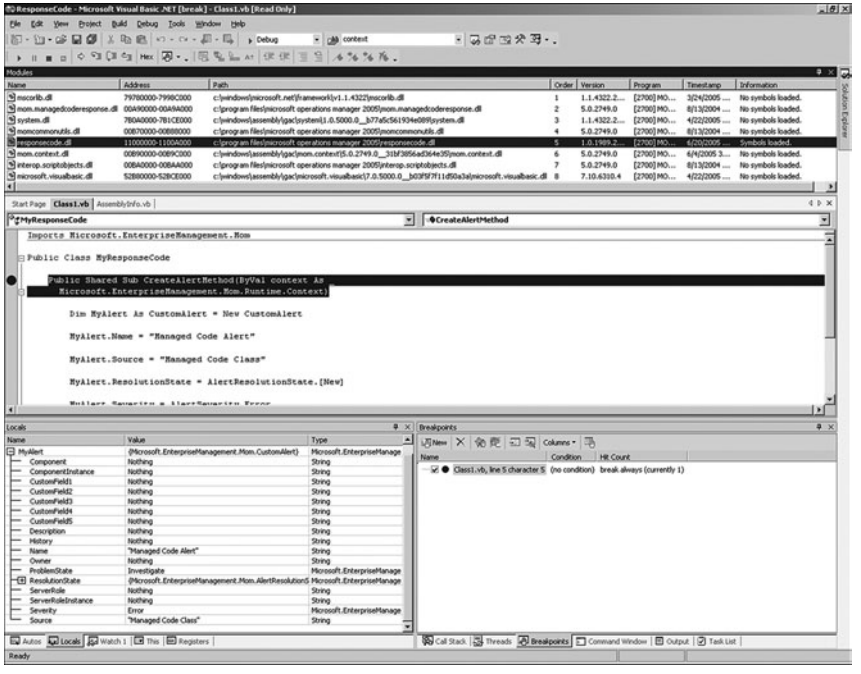


FIGURE 22.11 Checking the managed code symbols.

Attaching Process Debugger

The MOM Host process loads the files required to run the managed code as needed. If no assemblies are currently running on the target system you may not be able to locate the MOM Host process responsible for running managed code responses. The MOM Host process may also be cycled in specific scenarios, such as when the system receives new rules. When the MOM Host process is cycled, the Visual Studio .NET debugging session attached to that process will also end.

This behavior is similar to that described in the "Locating the Correct MOM Host Process" sidebar in the "Debugging Scripts" section of this chapter.

Tools

A variety of tools are available to assist you with using and developing scripts in MOM. Some of these include

- MOM 2005 SDK—The Microsoft Operations Manager 2005 SDK documentation is useful when developing custom response scripts and managed code assemblies. This document provides additional examples for each of the objects and classes in the MOM scripting library and the MOM runtime namespace. The SDK documentation is also a useful reference for detailed information on the MOM .NET Framework Class Libraries if you are interested in developing external applications and connectors that interface with MOM.
- MOM 2005 Resource Kit tools—The Microsoft Operations Manager 2005 Resource Kit tools are essential for testing your MOM implementation. The resource kit includes tools such as the Event Creator and the Managed Code Runtime Utility. The Event Creator can generate synthetic events in the event log, which comes in handy when testing rules that trigger custom response code. The Managed Code Runtime Utility allows you to get properties of the assembly files, which are required to configure the response rule within the MOM Administrator console. Both the MOM 2005 SDK and the MOM Resource Kit tools are available at http://www.microsoft.com/Mom/downloads/2005/default.mspx.
- Response Test utility—Microsoft added a new tool to the MOM 2005 SP1 version of the resource kit. The Response Test utility allows executing MOM scripts outside the MOM runtime to assist in the debugging process.
- Visual Studio .NET—Visual Studio .NET 2003 is required when developing managed code assemblies for use as rule responses. The set of tools provided with the Visual Studio .NET suite are also useful when debugging your scripts and managed code.
- SMS Trace—The SMS Trace utility is a real-time log viewer. This utility is handy because you can keep the trace log file opened on the target system and watch the trace information scroll through the display window.

Runtime Scripting Objects

This section lists the objects along with the methods and properties associated with each object in the MOM scripting library. For additional information on how to use each of these objects within a script, refer to the earlier section "Creating a New Script" and the Microsoft Operations Manager SDK.

Used by the Response Script

Response scripts use the ScriptContext object to interact with the various elements found within MOM including alerts events, performance data, discovery information, and variable sets. When custom response scripts are created the ScriptContext object is used to interact with other objects found in the scripting library to achieve interaction with MOM and the various data types.

Alert Object

The ScriptContext.CreateAlert() method is used to create a new instance of the Alert object. After a new instance of the Alert object is created, the properties and methods associated with the Alert object can be used to configure the alert details. When configuring the alert details, the AlertLevel, ProblemState, and ResolutionState properties require the numeric equivalent and not the name of the value. Review previous examples in this chapter and the MOM 2005 SDK for a list of values these properties can accept.

The ScriptContext.Alert property can be used to get an instance of the Alert object that triggered the script. After the instance of the Alert object is retrieved, the properties and methods associated with the Alert object can be used to retrieve details about the alert. The AddHistory and SetCustomField methods can update information on the original event. All other values are read-only when retrieving information about the event that triggered the script. Review Table 22.4 for a listing of the methods and properties available in the Alert object.

TABLE 22.4 `Alert` Object Methods and Properties

Method Name	Returns	Property Name	Returns
oAlert.AddHistory(*string*)	—	oAlert.AlertLevel	Long
oAlert.GetCustomField(*field #*)	String	oAlert.AlertSource	String
oAlert.SetCustomField(*field #*, *string*)	—	oAlert.Component	String
		oAlert.ComponentInstance	String
		oAlert.Computer	String
		oAlert.ComputerDomain	String
		oAlert.Description	String
		oAlert.ID	String
		oAlert.Name	String
		oAlert.Owner	String
		oAlert.ProblemState	Long
		oAlert.ResolutionState	Long

TABLE 22.4 Continued

Method Name	Returns	Property Name	Returns
		oAlert.ServerRole	String
		oAlert.ServerRoleInstance	String
		oAlert.UTCTimeOfFirstEvent	Date
		oAlert.UTCTimeOfLastEvent	Date

Event Object

The ScriptContext.CreateEvent() method is used to create a new instance of the Event object. After a new instance of the Event object is created, the properties and methods associated with the Event object are available to configure the event details. When configuring event details, the EventType property requires the numeric equivalent and not the name of the value.

The ScriptContext.Event property can be used to get an instance of the Event object that triggered the script. After the instance of the Event object is retrieved, the properties and methods associated with the Event object can be used to retrieve details about the event. All values are read-only when retrieving information about the event that triggered the script. Review Table 22.5 for a listing of the methods and properties available in the Event object.

TABLE 22.5 `Event` Object Methods and Properties

Method Name	Returns	Property Name	Returns
oEvent.EventParameter(*ParmID*)	String	oEvent.Category	String
oEvent.SetEventParameter(*string*)	—	oEvent.EventNumber	Long
		oEvent.EventParameterCount	Long
		oEvent.EventSource	String
		oEvent.EventType	Long
		oEvent.ID	String
		oEvent.LocalTime	Date
		oEvent.LoggingComputer	String
		oEvent.Message	String
		oEvent.MessageDLL	String
		oEvent.SourceComputer	String
		oEvent.SourceDomain	String
		oEvent.UTCTime	Date
		oEvent.UserDomainName	String
		oEvent.UserName	String

PerfData Object

The ScriptContext.CreatePerfData() method creates a new instance of the PerfData object. After a new instance of the PerfData object is created, you can use the properties associated with the PerfData object to configure the performance details.

The ScriptContext.PerfData property can be used to get an instance of the PerfData object that triggered the script. After retrieving the instance of the PerfData object, the properties associated with the PerfData object can be used to retrieve details about the performance data. All values are read-only when retrieving information about the performance data that triggered the script. Review Table 22.6 for a listing of the properties available in the PerfData object.

TABLE 22.6 PerfData Object Properties

Property Name	Returns
oPerfData.CounterName	String
oPerfData.ID	String
oPerfData.InstanceName	String
oPerfData.ObjectName	String
oPerfData.SampleLocalTime	Date
oPerfData.SampleUTCTime	Date
oPerfData.SourceComputer	String
oPerfData.SourceDomain	String
oPerfData.Value	Long

Rule Object

The ScriptContext.Rule property can be used to get an instance of the Rule object that triggered the script. You can then use the properties associated with the Rule object to retrieve details about the rule. Both properties are always read-only when retrieving information about the rule that triggered the script. Review Table 22.7 for a listing of the properties available in the Rule object.

TABLE 22.7 `Rule` Object Properties

Property Name	Returns
oRule.ID	String
oRule.Name	String

ScriptState and VarSet Objects

The ScriptContext.GetScriptState() method can be used to interact with the VarSet object. The VarSet object can be used by the script to store variables on the target system. Review Tables 22.8 and 22.9 for a listing of the methods and properties available in the ScriptState and VarSet objects.

TABLE 22.8 ScriptState Object Methods

Method Name	Returns
oScriptState.CreateSet()	Object
oScriptState.DeleteSet(*String*)	—
oScriptState.GetSet(*String*)	VarSet
oScriptState.SaveSet(*VarSet, Object*)	—

TABLE 22.9 VarSet Object Methods

Method Name	Returns
oVarSet.DumpToFile(*String*)	File
oVarSet.get(*String*)	VarSet
oVarSet.put(*String, Value*)	—

Discovery Objects

The ScriptContext.CreateDiscoveryData() method can be used to work with the DiscoveryData objects within the MOM scripting library. Review Tables 22.10 through 22.15 for a listing of the methods and properties available in each DiscoveryData object.

TABLE 22.10 DiscoveryData Object Methods and Properties

Method Name	Returns	Property Name	Returns
oDiscData.AddCollection(Object)	—	oObject.ScopeID	String
oDiscData.CreateRelationshipCollection()	Object		
oDiscData.CreateCollection()	Object		

TABLE 22.11 DiscoveryCollection Object Methods and Properties

Method Name	Returns	Property Name	Returns
oDiscColl.AddInstance(Object)	—	oDiscColl.ClassID	String
oDiscColl.AddScopeComponent(String)	—		
oDiscColl.AddScopeFilter(sKey, sValue)	—		
oDiscColl.AddScopeProperty(String)	—		
oDiscColl.CreateInstance()	Object		
oDiscColl.DisableScope()	—		

TABLE 22.12 DiscoveryRelationshipCollection Object Methods and Properties

Method Name	Returns	Property Name	Returns
oDiscRel.AddInstance(*Object*)	—	oDiscRel.TypeID	String
oDiscRel.CreateInstance()	Object	oDiscRel.TargetScopeFilter	Object
oDiscRel.DisableScope()	—	oDiscRel.SourceScopeFilter	Object
oDiscRel.AddScopeProperty(*String*)	—		

TABLE 22.13 DiscoveryClassInstanceID Object Method

Method Name	Returns
oDiscCI.AddKeyProperty(s*Key, s*Value*)	—

TABLE 22.14 DiscoveryInstance Object Methods

Method Name	Returns
oDiscInst.AddComponent(s*ID*)	—
oDiscInst.AddKeyProperty(s*ID, sValue*) sValue)	—
oDiscInst.AddProperty(s*ID, sValue*)	—

TABLE 22.15 DiscoveryRelationshipInstance Object Methods and Properties

Method Name	Returns	Property Name	Returns
oDiscRI.AddProperty(s*ID, sValue*) ss*sValue*)	—	oDiscRI.SourceProperty	Object
oDiscRI.AddProperty(s*ID, sValue*) ss*sValue*)	—	oDiscRI.TargetProperty	Object

Summary

MOM 2005 offers exceptional monitoring capabilities right out of the box. For most organizations, custom monitoring scenarios aren't considered out of the ordinary but more commonplace because they exist throughout the enterprise. Fortunately, the functionality within MOM can be adapted to almost any environment by developing and implementing custom script and managed code responses. These custom responses can be simple to implement and can work with the environment you are monitoring and all the different elements found in MOM. The next chapter provides an overview of Microsoft's direction in monitoring with a tour of Operations Manager 2007!

CHAPTER 23

Touring Operations Manager 2007

IN THIS CHAPTER

In 2005 Microsoft began development work on the next version of Operations Manager, initially code-named MOM V3, renaming it in 2006 to System Center Operations Manager 2007. As we are completing this book, the newest version of Operations Manager is in beta test, with general availability projected for 2007.

This chapter gives an overview of Operations Manager 2007 as it is in this stage of its development, and discusses its placement within the rapidly growing and evolving System Center family of management applications. We will talk about strategy for moving from MOM 2005 to the new management paradigm, and look at some new technologies previewed in the beta version of Operations Manager 2007 (also known as Ops Manager 2007 or OpsMgr 2007).

Prerelease Software

Everything is this chapter is based on prerelease "beta" documentation and software from Microsoft and is therefore subject to change in future release candidate and production versions.

We can describe Operations Manager 2007 in three words: *easy scalable knowledge*. Microsoft amassed a tremendous amount of customer and partner feedback about MOM 2005, and OpsMgr 2007 responds to industry-driven inputs with some profound innovations in the Microsoft management space:

- Easy—The former three consoles of MOM 2005 (Administration, Reporting, and Operations) become a single console with OpsMgr 2007, simplifying the user interface.

- Scalable—For organizations deploying computers via images, OpsMgr 2007 lets you assign computers to management groups via Active Directory. A base OpsMgr 2007 agent can be preinstalled on computers, and when those computers "wake up" with their permanent name and role, they automatically attach to their preassigned management group and begin reporting.
- Knowledge—This has always been Microsoft's greatest strength with the MOM product, with knowledge encapsulated in management packs. Operations Manager 2007 introduces the concept of sealed management packs. Management packs from Microsoft and other vendors are sealed, versioned, and signed with a certificate. After a management pack (MP) is imported you begin adding knowledge to it, saving the changes separately. Importing a new version of the management pack replaces the superseded version of the vendor management pack, but company knowledge is retained intact.

Microsoft System Center Evolution

After several years of evolution, Microsoft System Center is finally showing itself as a respectable management technology framework in its own right. In conjunction with this development, Microsoft is positioning System Center Operations Manager 2007 as the core component in an enterprise deployment of System Center (SC) applications. These are heartening advances for Windows networking professionals because the existence of reliable and effective native Microsoft management tools can increase and protect the value of Microsoft technology investments for everyone.

SC applications include the capability to share databases and interoperate with each another for scalability and adaptability. In Chapter 1, "Operations Management Basics," we cited an early demonstration of this synergy with the capability of SC Reporting Manager 2006, which can correlate information about both MOM and Systems Management Server (SMS) when both systems are installed. Other System Center applications in development include:

- SC Configuration Manager (which replaces SMS) and an application code-named SC "Service Desk" are big pieces of Microsoft's SC solution for the enterprise. We discuss SC Configuration Manager and Service Desk further in the next section of this chapter.
- SC Virtual Machine Manager is currently a beta product in the SC family. Microsoft designed Virtual Machine Manager to increase physical server utilization by consolidating virtual infrastructures and centralizing management of virtual machines (VMs). Because VMs are created out of existing pockets of excess storage and RAM, it's great to be able to manage those virtualized resources confidently across many systems.
- SC Essentials or SCE (pronounced *ski*) is a System Center beta application for the small to medium business that combines the monitoring features of SC OpsMgr with the inventory and software distribution functions of SC Configuration

Manager. SCE has some surprising features, which we discuss later in the "System Center Essentials 2007" section of this chapter.

Some likely synergy between the SC offerings appears to include SC Configuration Manager and SCE sharing some technology for distributing software updates, SC OpsMgr and SCE sharing similar agent technology, and SC "Service Desk" sharing databases with SC OpsMgr and SC Configuration Manager.

OpsMgr 2007 is positioned as a major "next generation" server application for Microsoft along with Exchange 2007, sharing new technologies such as PowerShell (Monad), discussed in the "Introducing New Technologies" section later in this chapter, and support for 64-bit x64 processors. Similar to the MOM 2005 Operator console, the OpsMgr 2007 console uses the popular Outlook interface with navigation panes and tiles, and adds tremendously customizable frames. The OpsMgr 2007 console has the polished look and feel of other contemporary Microsoft products, such as Microsoft ISA Server 2006. An added valuable benefit shared by OpsMgr 2007 and newer Microsoft server applications is the automatic delivery of software updates via technologies such as Microsoft Update and Windows Server Update Services (WSUS).

SC Configuration Manager 2007 and SC "Service Desk" Applications

There are at least three major components of the System Center suite to consider evaluating for deployment in 2007. In addition to SC Operations Manager, we suggest the SC Configuration Manager and SC "Service Desk" applications as prime candidates for consideration.

SC Configuration Manager 2007

Microsoft has rebranded the SMS v4 product as SC Configuration Manager (SCCM), Microsoft's renamed and revamped systems management solution for change and configuration management. Features available for evaluation in the SCCM 2007 beta release include the following:

- Network Access Protection (NAP) is a policy enforcement platform built into the Microsoft Windows Vista and Windows Server "Longhorn" operating systems. NAP helps protect network assets by enforcing compliance with system health requirements, including enforcement across most common network access scenarios. This technology extends the Quarantine Access Control solution, previously only applicable in Microsoft Virtual Private Network (VPN) scenarios, to wired and wireless computers on the Local Area Network (LAN) including clients using Dynamic Host Configuration Protocol (DHCP) for Transmission Control Protocol/Internet Protocol (TCP/IP) address assignment.
- Operating system deployment using the new Windows Image (.WIM) file format. This technology is based on the Operating System Deployment (OSD) Feature Pack currently available for SMS 2003 SP1.

- Simplified User Interface (UI) including enhanced multiple selection and drag-and-drop operations.
- Software updates no longer use the legacy SMS software distribution components (packages, programs, and advertisements) when distributing software updates to clients. SC Configuration Manager now creates software update packages using simpler native technologies.
- For software distribution, branch distribution points allow small office locations to host software packages on workstation computers without requiring the equivalent of an SMS secondary site. Package transfers to the branch distribution points trickle across the corporate Wide Area Network (WAN) or VPN according to bandwidth-controlled settings using BITS (Background Intelligent Transfer Service).

SC "Service Desk"

A Microsoft System Center component for IT Service Management, code-named "Service Desk," is currently under development. SC "Service Desk" implements a single point of contact for all service requests, knowledge, and workflow. The Service Desk incorporates processes such as incident, problem, change, and asset management.

Just as OpsMgr is master of the Microsoft Operating Framework (MOF) Operating Quadrant, Service Desk will be an anchor for the MOF Supporting Quadrant. Figure 23.1 illustrates the mapping between the quadrants of the MOF Process Model and System Center Components.

The "Service Desk" is a new Microsoft help desk product and fills a gap in both MOM 2005 and OpsMgr 2007: What do we do when MOM 2005 or OpsMgr 2007 detects a condition that requires human intervention and tracking to resolution? Until "Service Desk," the answer was to create a ticket or incident in our help desk application. Now, within the SC framework, SC OpsMgr can hand off incident management to SC "Service Desk."

Design goals of "Service Desk" include the following:

- Utilizing Microsoft technologies that people already use or are familiar with; for example, "Service Desk" uses the SharePoint and InfoPath products for web portal and knowledge base functions.
- Incorporating Self-Service Portal technologies to help organizations reduce support costs, including providing the administrator with visibility into the overall performance of the IT environment using reports and dashboards.
- Ready to use process-automated workflows based on the Microsoft Operations Framework.
- An SC "Service Desk" Solution Pack framework, similar to the SC Operations Manager Management Packs, enables customers and partners to develop additional custom functionality for "Service Desk."

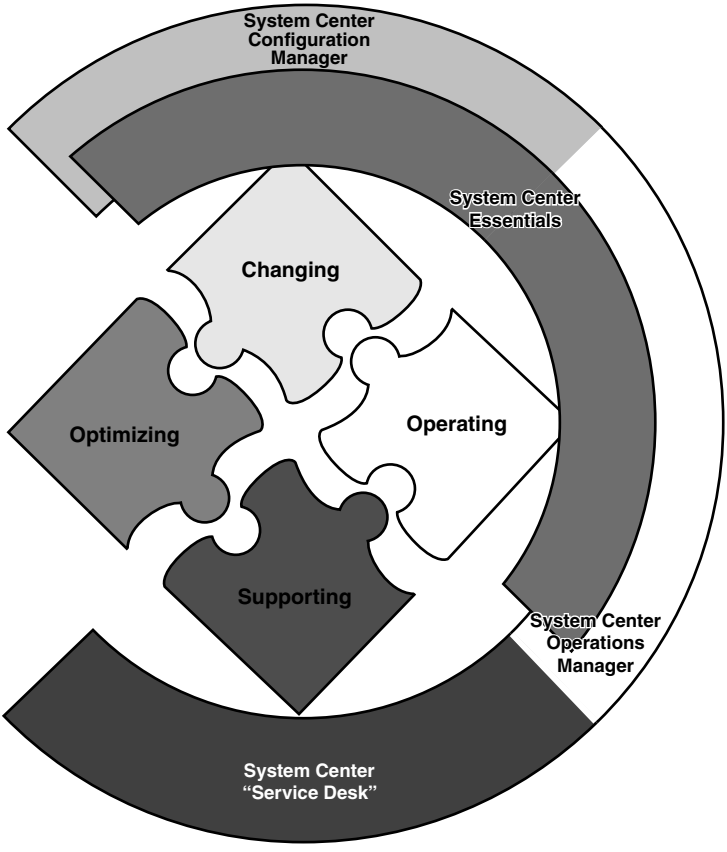


FIGURE 23.1 MOF quadrants and "next generation" System Center applications.

- A Configuration Management Database (CMDB) based on System Definition Model language.

SC "Service Desk" supported scenarios include the following Service Management Functions (SMFs) and capabilities from the MOF Operating and Supporting Quadrants:

- Incident management—Creating incident records based on information in management tools
- Problem management—Identifying problems by searching common incidents
- Asset management—Tracking movement and ownership of hardware assets
- Change management—Reviewing and approving Change Requests
- Self- Service Portal—Resolving an issue without calling the Service Desk

Aligning OpsMgr 2007 with ITIL and MOF

The Information Technology Infrastructure Library (ITIL) and MOF are all about process-based techniques that exist to deliver specific applications and services—*It's the applications and services* that matter in MOF, and OpsMgr 2007 is well focused in that regard. OpsMgr 2007 will help IT decision-makers start thinking and acting in terms of services rather than servers, and of end-to-end application functionally in addition to router-to-router site connectivity. Previously inscrutable MOF quadrants and SMFs can start to make sense to managers with live, meaningful dashboards and monitors in OpsMgr 2007 that validate the logic of using MOF as the basis in network management.

Standard service level definitions, including metrics reporting, are the key to unambiguous services delivery. With OpsMgr 2007's new sealed management pack concept and streamlined tuning, SC Operations Manager 2007 creates a vehicle for the definition and scope of Service Level Agreements (SLAs). Microsoft's new approach of *code signing*, sealing the MP with a certificate, is the management pack author's assurance that the MP contains reasonable thresholds for acceptable performance. For example, a vendor-supplied, sealed MP managing a standard service on any number of servers results in utilitylike delivery of a "commodity" of known quality.

The people, processes, and technologies that make up the Information Technology (IT) Service Management discipline are the definition of a massively complex system. Viewing IT challenges and opportunities through the lenses of the MOF quadrants augments the human mind with a framework for making good IT-related decisions. Microsoft System Center management products such as OpsMgr 2007 enable best practice support to manage the dozens of IT SMFs. A well-designed SC solution that includes OpsMgr and Service Desk sealed management packs and knowledge offers the promise of what we might call a real "MOF in a box" solution!

Strategic Deployment Considerations

OpsMgr 2007 is in some ways a first version product for Microsoft. MOM 2000 and 2005 owed much of their origin to the NetIQ and Mission Critical Software management product lines, such as the OnePoint service and database. Microsoft is now taking full ownership of the former NetIQ and Mission Critical technologies. Although it keeps the well-behaved, small footprint agent for both the SC OpsMgr and SC Essentials products, OpsMgr 2007 is a different product than MOM 2005 and its predecessors on the backend, console UI, and features side.

We see this as a positive step because through its experience with the SMS product, Microsoft (and the Microsoft management community) endured the consequences of holding onto stale technologies. SMS 2003 in the year 2006 uses the same basic software distribution technology as the SMS 1.0 product developed more than a decade ago, a technology with a lot of overhead that is no longer necessary. With the release of SC Configuration Manager 2007 Microsoft is finally retiring most of the legacy SMS technology.

Microsoft has used the period since introducing MOM 2000 for collecting and analyzing data with the goal of perfecting management of Windows-based services and applications. To avoid technological dead ends, Microsoft decided to make OpsMgr 2007 more than just an evolution of an existing product—it changed the guts! Microsoft has a vision and it is going to impart that vision to us.

The main components of OpsMgr 2007, namely the OpsMgr Management Server application and the OpsMgr Console, are all-new constructions and are a complete departure from previous versions of the product. However, OpsMgr 2007 does build on previous MOM agent technologies and continues to utilize SQL Server Reporting Services for OpsMgr Reporting.

Transitioning from a Microsoft Operations Manager 2005 Ecosystem

Users of MOM 2000 migrated to a fairly familiar platform, MOM 2005, which retained most of MOM 2000's architecture and then improved it. The result was a robust management system that has become the world's premier platform for Windows server management. The result was also the complex, sometimes overwhelming, assemblage of knowledge and data collection about server-centric processes that is MOM 2005.

The global MOM Community has really come together to create the "MOM Ecosystem," which is the network of individuals, partners, and allied technologies that support and extend the MOM framework. With healthy competition plus an ever-broadening scope of offerings, hundreds of software shops, large and small, help organizations in extending and enhancing the functionality of MOM 2005. In addition, most if not all leading application vendors, such as Citrix and VERITAS (Symantec), position MOM as a supported and often preferred means of monitoring the performance of their applications.

There is little doubt that investments in Microsoft System Center technologies such as Operations Manager are sound; there is no reason to consider other platforms to monitor and manage Microsoft servers. MOM 2005 is the zenith of server-centric Microsoft management technologies and will probably remain a market leader well into 2008. There is nothing wrong with MOM 2005—it is not broken and being fixed by OpsMgr 2007. MOM 2005 is a fantastically stable, reliable, and scalable platform. This was not the case with MOM 2000, which was in desperate need of an upgrade by the time MOM 2005 became available.

We recommend that enterprises without Operations Manager implement MOM 2005 now and not wait for SC OpsMgr 2007. Microsoft recommends, and we concur, that new customers interested in OpsMgr 2007 install MOM 2005 now to collect data to use in later building the application-specific Line of Business (LOB) Monitors in OpsMgr 2007.

Microsoft will support a direct migration from MOM 2005 to OpsMgr 2007. However, the new Management Server, Console, and Connector technologies in OpsMgr 2007 indicate that organizations might better consider the process a "conversion" to OpsMgr 2007 rather than "migration" from MOM 2005. We can anticipate a period of several years before native OpsMgr 2007 Management Packs are widely available. Large IT shops will

need some time to gain confidence and comfort with the new paradigm of OpsMgr 2007. One logical migration plateau might be to keep using MOM 2005 for base OS management to meet near-term server-based SLAs while shifting primary emphasis for application management to OpsMgr 2007, developing the application-based SLAs that organizations are really seeking.

Adopting SC OpsMgr 2007 can be an opportunity and occasion to depart from legacy network monitoring tools and methodologies. It will take some time to develop and appreciate skills such as converting to new application-centered network topologies and designing integrated multidiscipline application monitoring processes.

Moving Toward Application-Centered Management

Large organizations traditionally observe and protect their investment using a router-centric, geographic network management map, such as Tivoli's Enterprise Console (TEC) or Hewlett-Packard's Network Node Manager (NNM). (Hopefully using product connectors to MOM 2005!) These traditional types of network maps verify that servers and their processes are running, and that the interconnecting routers, firewalls, and switches are error-free. However, this approach does not necessarily guarantee that the application(s)—the reason the networks exist—are actually delivering the necessary business functions to their human and automated constituents.

For example, a typical SLA to host or manage Exchange Server is often validated by processes confirming that the Exchange Server hardware and software continues to run normally (such as the MOM 2005 Base OS and other MPs), and checking whether mail is moving in and out of the server (like the Exchange management pack mail flow). We can illustrate principal limitations to this traditional approach with the following challenges:

- Distributed applications running on many physical tiers can be difficult and time consuming to manage. Different teams of people, such as different Network Operations Centers (NOCs), or different Subject Matter Experts (SMEs) must communicate and cooperate to keep these applications running. For example, an Exchange SLA might depend on the function of a third-party security appliance managed by a different team or company.
- Instrumented testing of email flow often uses a technology dissimilar to the email client technologies that network users typically depend on to perform their work. Even the synthetic Messaging Application Programming Interface (MAPI) logons performed by the MOM 2005 Exchange MP, for example, are not capturing the complete experience a user has running Outlook 2003 in Exchange Cached Mode using Remote Procedure Calls (RPC) to communicate across HTTPS over the Internet. If a business depends on this user scenario, its best Exchange SLA is one that monitors the availability and usefulness of that particular scenario.
- The abstraction of networks in the form of router-based point-to-point hierarchical maps of servers and their roles can shift the focus too far away from the applications for which the network exists in the first place. Decisions are made that support the infrastructure rather than the Line of Business.

We can make better tactical and strategic decisions when visualizing the network and its health as services and applications of certain capacities and limitations. Cross-platform event correlation—the Nirvana of enterprise network management and a requirement for truly effective distributed application monitoring—becomes easier when all of an application's physical and virtual underpinnings are intelligently laid out for the decision-maker. OpsMgr 2007 is "abstracting" us up to a new level in our thinking—as we outgrow our server-centric management world and seek holistic and common sense ways to do our jobs better.

Introducing New Technologies

The "look and feel" of System Center Operations Manager 2007 is quite a departure from the previous version, MOM 2005. Even longtime MOM administrators need some wandering-around time in the redesigned single console to get their bearings. This section includes some screen shots and a short discussion of selected new features in OpsMgr 2007.

Single Console with a Dashboard Overview

Previous versions of MOM required multiple consoles to use the product. MOM 2000 had two consoles (Management console and Reporting console), and MOM 2005, by splitting out the administration features to their own console, had three consoles. OpsMgr 2007 has only one Management console that combines the three consoles of MOM 2005. Previous versions of MOM also included a web-based Operations console. (There is no Web console included with the Beta 2 version of OpsMgr 2007, although Microsoft plans to include one with the final product.)

In OpsMgr 2007 all administration, monitoring, and reporting functions take place using this single console. Figure 23.2 shows the top-level view of the Monitoring section of the OpsMgr 2007 console. The console has a primary top-level Monitoring view including some dashboard features. Dashboard features previewed in the beta edition of OpsMgr 2007 include counters of alerts received today by severity and source, and a meaningful graph showing new versus resolved alert trending over the last four days.

The lower left side of the OpsMgr 2007 console has tiles that you click to move between the five major console workspaces: Monitoring, Authoring, Reporting, Administration, and My Workspace. Here is how these workspaces map to their MOM 2005 console counterparts:

- Monitoring—Corresponds to the MOM 2005 Operations console; this is where most work takes place.
- Authoring—This is where some of the rule and computer group functions of the MOM 2005 Administration console have migrated.
- Reporting—Similar to the MOM 2005 Reporting console, accessed from within the main OpsMgr console.

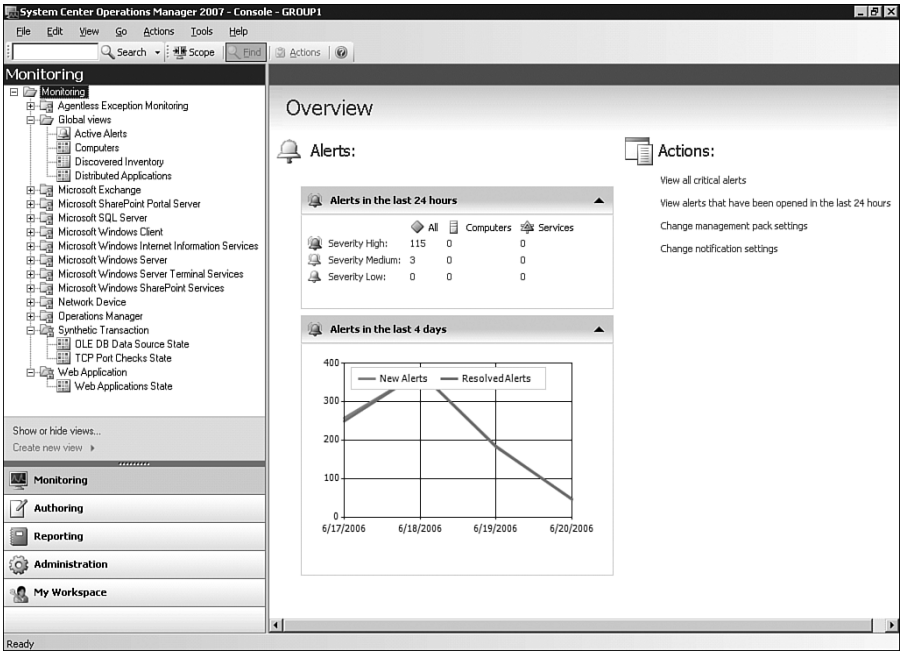


FIGURE 23.2 OpsMgr 2007 top-level Monitoring Overview with dashboard features.

- Administration—The remainder of the MOM 2005 Administration console functions that did not move to the OpsMgr 2007 Authoring Workspace, such as discovery and notification settings.
- My Workspace—Similar to the My Views folder in the MOM 2005 Operations console; this is where to access your personal favorite views and saved searches.

We will look at several of these new workspaces in this chapter, but first we'll take note of some of the new features and capabilities on the Monitoring console. Figure 23.3 shows the OpsMgr 2007 Beta 2 view that most closely resembles the Computer Groups/All Computers view frequently used in MOM 2005 for monitoring operations.

Something you will notice missing in the new OpsMgr 2007 Monitoring console is the distinctive State Indicator toolbar with its count of the number of servers managed in the red, yellow, and green states unique to the MOM 2005 Operations console. If you still want counters in OpsMgr 2007, they are available on the Monitoring Overview dashboard displayed in Figure 23.2. A possible reason for the retirement of the state indicator comes to mind when we study a terrific new feature of the console, which is the ability to group and nest managed objects in the primary frame.

Figure 23.3 shows the alerts grouped first by severity, then by Maintenance Mode status, and finally sorted by time received. An additional level of subgrouping is possible for a maximum of three nested grouping criteria. Inset in the lower right of the screen is the Select Columns dialog box where you can see how easy it is to select columns to display

and present data in the most useful manner. In the corresponding MOM 2005 view, objects were in a flat view that sorted by columns only—a single-layer management space where a simple state counter was useful for event triage.

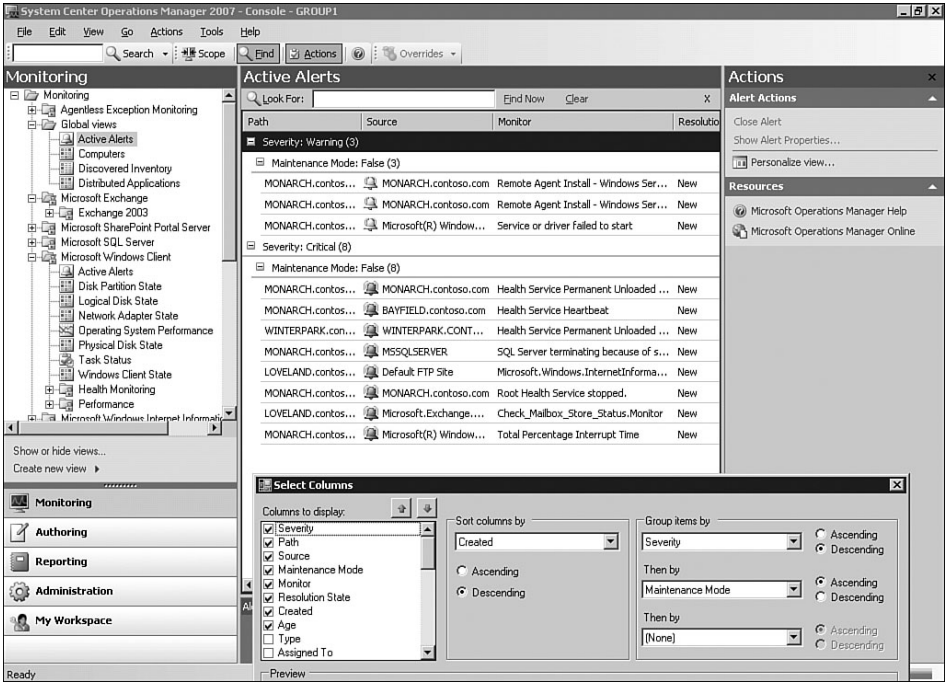


FIGURE 23.3 OpsMgr 2007 Active Alerts in the Global view of the OpsMgr 2007 Monitoring console.

The central portion of the OpsMgr 2007 console has an all-new flexibility to reconfigure and display information in up to six different panes. In Figure 23.4, the top center of the Monitoring Workspace automatically divides into two panes to show the Agent State as viewed from the management server and as viewed by the agent itself.

The upper right of Figure 23.4 shows the Start Maintenance Mode state action, launched using the Actions menu against a managed object. OpsMgr 2007 enhances the Maintenance Mode function introduced in MOM 2005 and common to other enterprise network management products.

Figure 23.5 displays the improved Maintenance Mode entry form launched from the Actions menu. The dialog box contains helpful information and lets administrators centrally document the reason for the maintenance. The administrator can also type a free-text comment that is accessible from all console views.

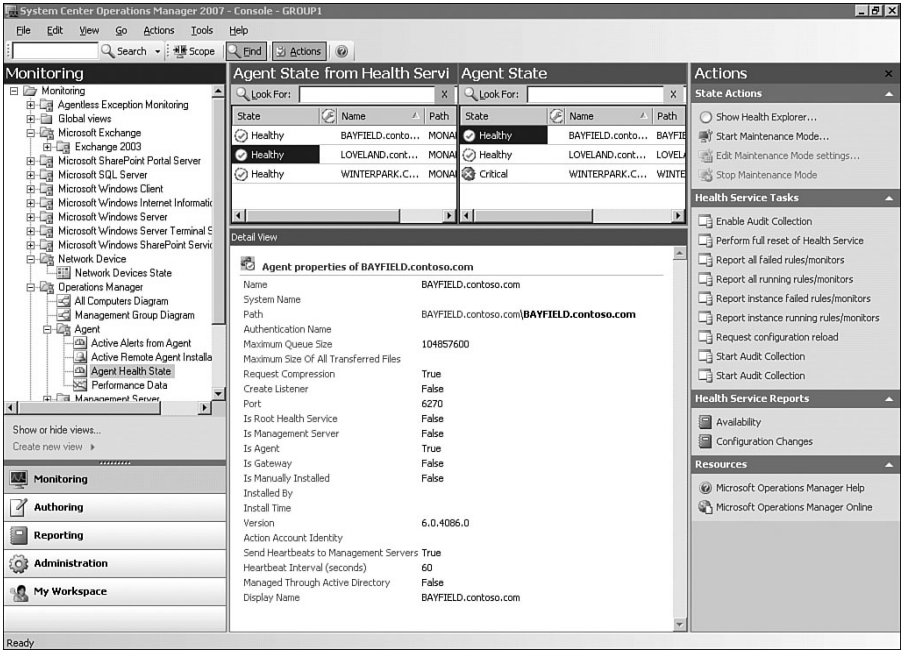


FIGURE 23.4 OpsMgr 2007 Operations Manager Agent state.

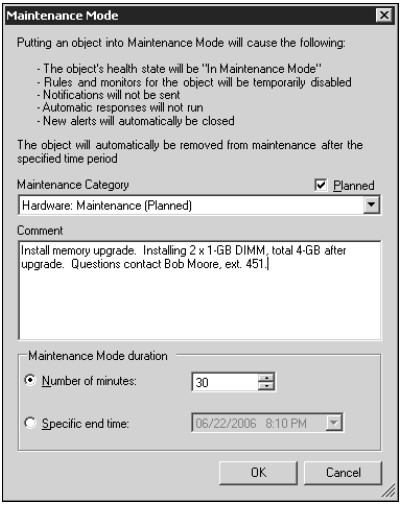


FIGURE 23.5 Placing a managed object into Maintenance Mode for scheduled hardware upgrade.

Maintenance Mode Capabilities

As discussed in Chapter 9, "Installing and Configuring Agents," MOM 2005 includes the capability to place a computer into maintenance mode. This is a useful feature but

does not allow you to put a component or part of the server in maintenance mode without putting the entire system into maintenance mode. For example, if your server has a failed component (say a single drive in a RAID5 array), it is not possible to place only the hardware in maintenance mode; maintenance mode would encompass the entire server including the operating system and installed applications.

At Microsoft's 2006 Management Summit (MMS 2006), there were discussions that maintenance mode could be enhanced to apply to particular components. This functionality is not included with Beta 2, and it is unclear if it will be part of the production release of Operations Manager 2007.

Now let's look at the FTP Site Monitoring view in Figure 23.6. The figure demonstrates an OpsMgr 2007 design goal of presenting useful information in the proper context without having to search or do a lot of mouse clicking. Notice the lower portion of the central pane with all the information about the Default FTP site nicely displayed, perhaps saving the administrator a Remote Desktop session to look at that information manually in the server's web services console.

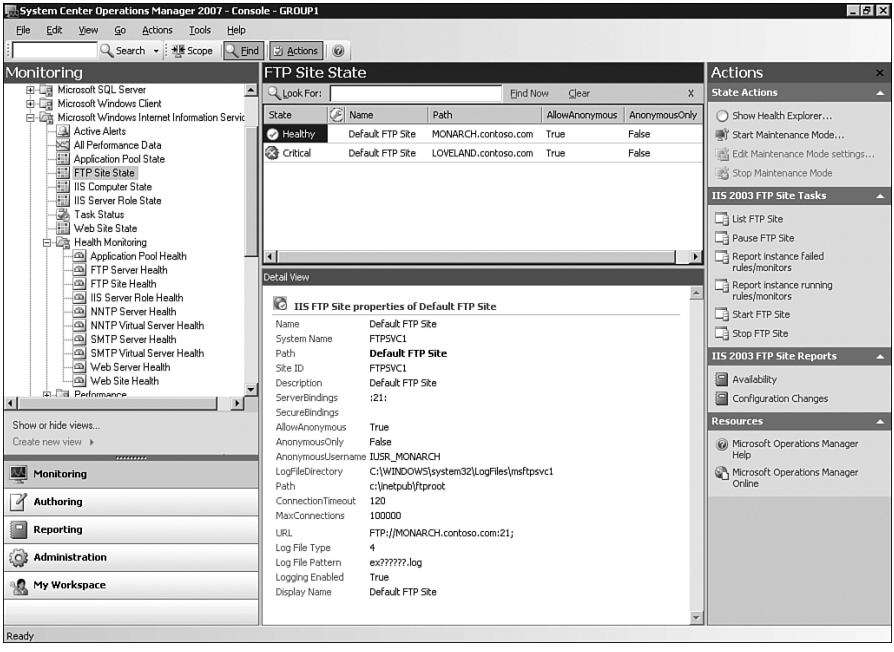


FIGURE 23.6 Monitoring FTP Site Health and configuration.

A useful feature in assisting with compliance and standardization is one allowing the administrator to create an ad-hoc matrix of configuration settings that detects anomalies and undesired settings that might affect service delivery. Look again at the right two columns in the center panel of Figure 23.6, AllowAnonymous and AnonymousOnly. We have personalized our view of the FTP Site State to include those columns because we want to track those security-sensitive settings.

New Health Monitor and Tools

In addition to the Start Maintenance Mode action, check the other action available in the State Actions panel, Show Health Explorer. Clicking this opens a new applet, the Health Explorer, which presents all the Health Monitors involved in determining the state of the managed object. *Health Monitors* are the OpsMgr performance counters, availability states, and other factors used to determine the health of an object. Figure 23.7 illustrates the Health Monitor launched from the Show Health Explorer Action in Figure 23.6 after selecting the Default FTP Site indicating a problem.

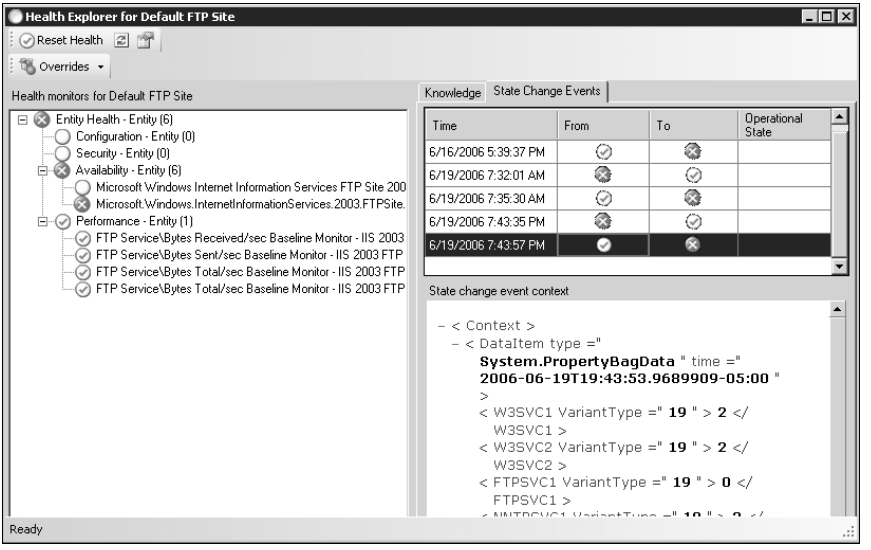


FIGURE 23.7 Health Monitor makes it easy to spot the problem, with clear state change history.

The left panel of Figure 23.7 displays Entity Health as a roll-up of one Availability monitor and four Performance monitors. This shows us at a glance how OpsMgr 2007 is assessing the health of an FTP site, and in the same glance which of those monitors are not healthy or green. The upper-right panel highlights another new feature—a visual record of the state change history of the selected monitor.

Also within the Health Explorer, the administrator can view Knowledge about the monitor and open an Alerts window with a list of all the actual alerts that affected Entity Health. The Overrides button at the top of the Health Explorer provides immediate access to Disable and Override criteria. The administrator can disable the monitor or override monitor characteristics for the selected object, for all objects of a certain type, or in a certain group. These are good innovations for enabling streamlined grooming and customization with OpsMgr 2007.

One-Click Performance Data Display

OpsMgr 2007 exhibits the ability of the new console in reconfiguring the workspace to communicate different types of information. In MOM 2005, performance graphics are somewhat isolated in their own workspace of the Operations console. Often, performance views of interest are nested deep within the rule hierarchy. After the desired performance rule is located, three steps are typically required to generate and display the graph.

In the new OpsMgr 2007 console, real-time graphical performance data is more accessible and usable because the performance views are now integrated into the console's Monitoring Workspace. For example, Figure 23.8 displays a chart of live web services performance data.

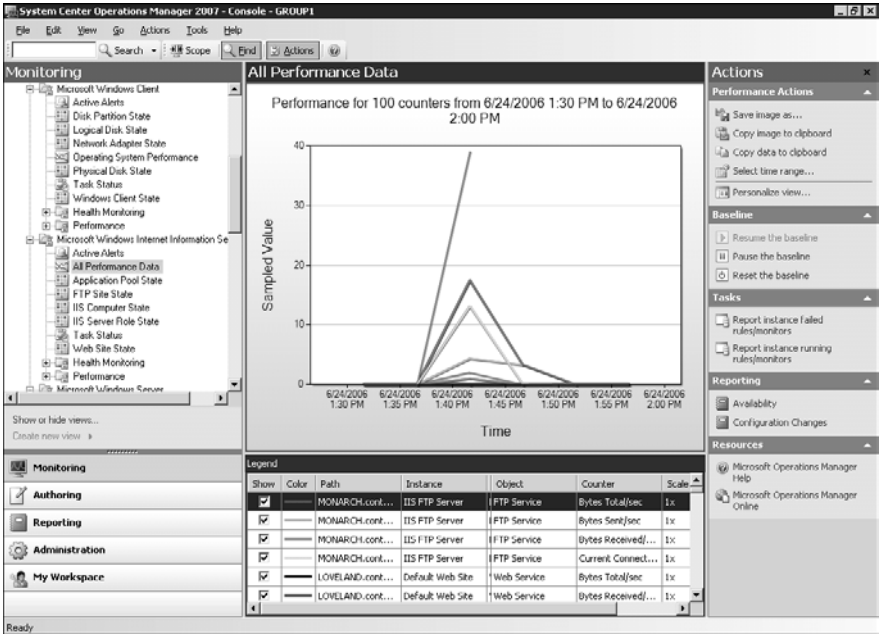


FIGURE 23.8 Live performance data graphics across multiple objects to spot correlations.

In Operations Manager 2007, selecting the Performance node of an application monitor displays the upper central portion of the console with one or more panes of blank graphs. The lower central portion lists available counters. These counters are by rows, with their line colors and other attributes and a blank check box beside each; clicking the check box instantly populates the selected graph with the charted data.

You can "paint" an ad-hoc multidimensional performance analysis one click at a time. For Figure 23.8, we selected all 100 available counters using the expected "right-click, select-all" that was available from the Legend row of the counters list, populating the graph almost instantly. In the upper-right Performance Actions section of Figure 23.8, you can see the one-click access to save the selected performance chart, copy the chart or its data to the Clipboard, modify the time range of the chart, or personalize the view.

A New Scripting Language, Windows PowerShell (Monad)

After completing setup of an OpsMgr 2007 management server, two program items are added to the Start menu under the System Center Operations Manager 2007 program group. One program item is the OpsMgr 2007 Operator console, which we have been examining, and the other item is the Command Shell. Additionally, a new program item is at the top level of the Start menu labeled Microsoft Command Shell. What shell is this and what can we do with it?

OpsMgr 2007 installs Windows PowerShell, formerly code-named "Monad," as an integral part of an Operations Manager installation. Although in a custom installation of OpsMgr 2007 you can deselect installing the Command Shell, it is generally a good idea to start learning about and working with the PowerShell.

PowerShell is the next generation Windows command shell. Both SC OpsMgr 2007 and Exchange 2007 utilize PowerShell. A design goal of PowerShell is to provide comprehensive control and automation of system administration tasks. Using PowerShell, you can use scripting to perform the most common actions a user might take in the OpsMgr 2007 console.

This command shell includes many concepts from traditional UNIX shells such as *bash* and *ksh*, and delivers text-processing support that has previously been a challenge with scripting languages such as Perl and Python. PowerShell builds on the .NET Framework as a fully object-oriented system. PowerShell requires .NET Framework 2.0, which is an installation prerequisite for OpsMgr 2007 management servers and is part of "Longhorn" Server.

Here are a few Command Shell views to help you appreciate the power and flexibility of this new object-managed shell. First, observe in Figure 23.9 the output of the Microsoft Command Shell from the `dir` command, when the shell context is file system objects. This looks like the file listing output using the familiar command shell Cmd.exe.

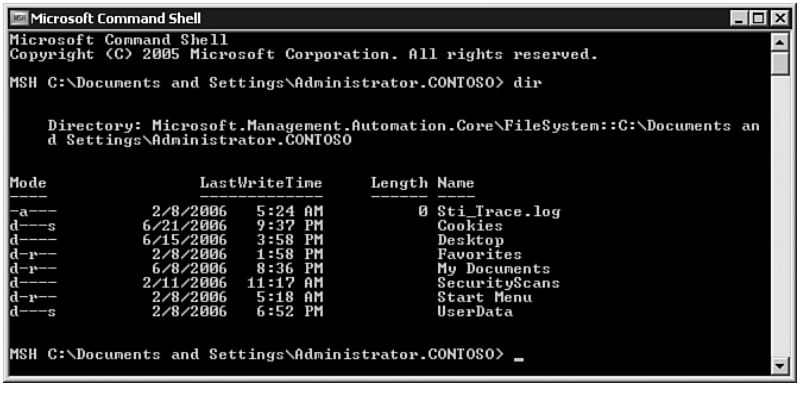


FIGURE 23.9 The `dir` output of Windows PowerShell, in the file system context, is similar to Cmd.exe.

The Command Shell window in Figure 23.10 shows an extract of a long `dir` output when the shell context is the Operations Manager 2007 Management Group. Observe that now the `dir` output format is a list of objects in the OpsMgr 2007 Group. We can act on the OpsMgr objects (such as computers, rules, groups, and distributed applications) as if they were files using familiar concepts such as copy and move.

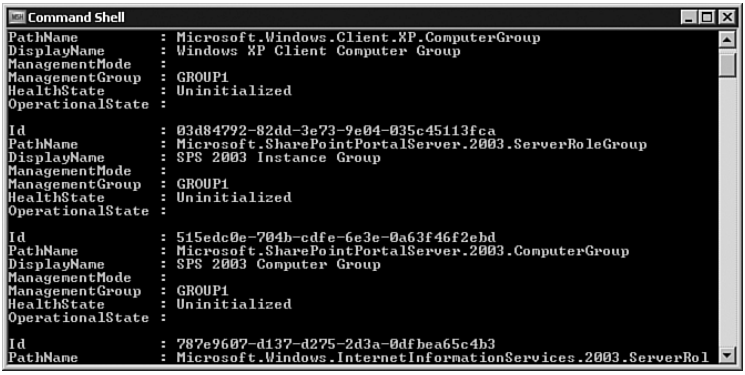


FIGURE 23.10 Bit of `dir` output of PowerShell when the context is the OpsMgr 2007 Management Group.

PowerShell also introduces a new Microsoft IT term, *cmdlet* (pronounced *command-let*). A cmdlet is the smallest unit of functionality in PowerShell and is analogous to the built-in commands of other shells. A cmdlet consists of a verb and noun pair, separated by a hyphen ("-").

Figure 23.11 shows some of the output of the PowerShell cmdlet `get-Command`. The `get-Command` cmdlet lists all cmdlets available given the shell's context. If you scan the list of cmdlets, you see OpsMgr cmdlet names such as `disable-Rule` and `approve-AgentPendingAction`, and you can visualize how we can manage and manipulate OpsMgr 2007 using scripted automation. This capability opens up worlds of possibilities for connecting to and interacting with System Center applications such as OpsMgr 2007.

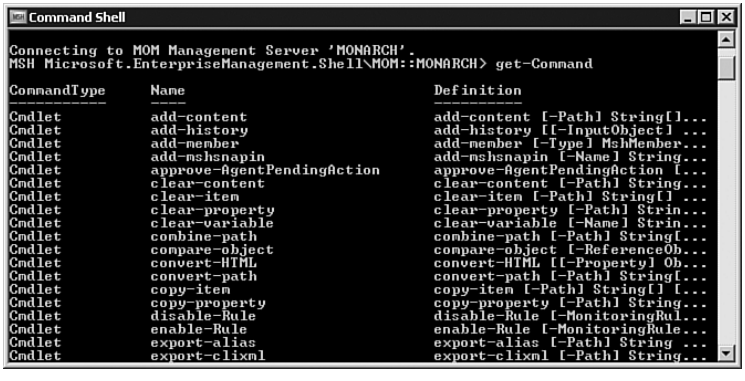


FIGURE 23.11 The cmdlet `get-Command` lists all the cmdlets available in the current context.

START USING WINDOWS POWERSHELL NOW

A Windows PowerShell version for x86, x64, and ia64 systems, which requires .NET Framework 2.0, is available for download. You can download the current version of the Windows PowerShell at http://go.microsoft.com/fwlink/?linkid=64772.

Agentless Exception Monitoring (AEM)

You may already be aware of Corporate Error Reporting (CER), a Microsoft application available to the enterprise administrator. CER uses the built-in Microsoft error reporting utility (Dr. Watson), which normally reports detailed error information anonymously to Microsoft over the Internet, also capturing that error information for analysis by the corporate IT shop.

Microsoft migrates the functionally of CER to the OpsMgr 2007 product, renaming the technology to Agentless Exception Monitoring (AEM). The word *agentless* emphasizes that within the System Center architecture, an installed agent is not required on a computer to benefit from this particular feature. AEM is a centralized low-hassle, in-house collection of Dr. Watson errors across all computers in the enterprise.

With AEM, an administrator using System Center Operations Manager 2007 can view solution responses to crashed applications investigated by Microsoft and/or partners. Within the System Center architecture, OpsMgr 2007 administrators host AEM for the enterprise, sharing system and application crash information with other administrators, even those that have no computers managed by Operations Manager.

Here is how it works: AEM uses an Active Directory (AD) Group Policy Object (GPO) to modify the behavior of the Dr. Watson utility running on computers that are members of the domain. On computers with this GPO applied, when a system crash occurs and a Dr. Watson event is generated, the crash analysis report is sent over the corporate network, WAN, or intranet to the OpsMgr 2007 management server(s) hosting the AEM service.

Implementing the many moving parts of AEM is pleasantly simple with OpsMgr 2007. A wizard launched from the OpsMgr 2007 console against one or more OpsMgr 2007 management servers opens an easy-to-use set of dialogs that configure and enable AEM. Figure 23.12 shows the wizard step where the administrator configures the client's error collection settings.

Usage of Port 6274

Pre-Vista computers send crash data to a file share; beginning with the Vista operating system, AEM client computers can optionally send crash data via SSL using port 6274.

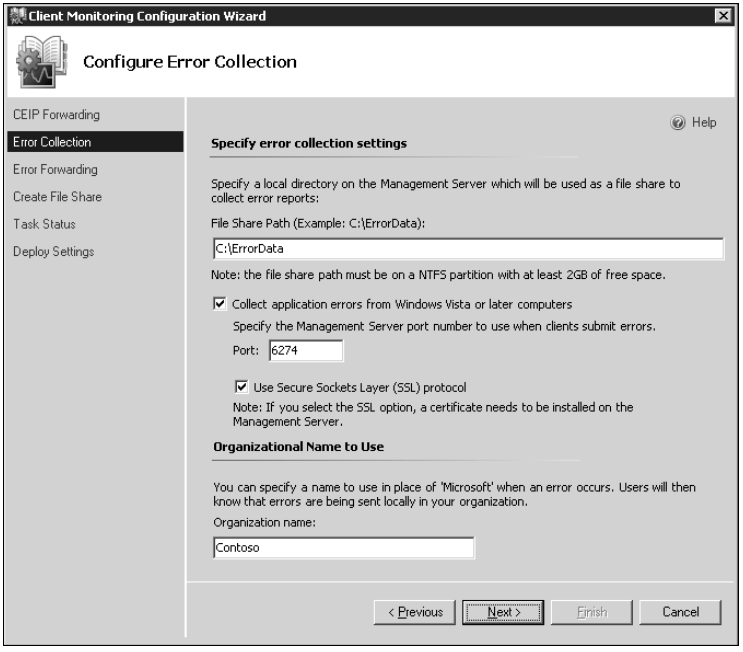


FIGURE 23.12 The step in the Enable AEM Wizard where the client's error collection settings are specified.

The final step of the Enable AEM Wizard creates a GPO Administrative Template file, AEM.adm, in a file folder location you specify. Default values for all the GPO settings involved in AEM are prepopulated with the settings entered with the Enable AEM Wizard. The AEM.adm file maintains any customizations.

You can use familiar AD tools such as AD Users and Computers and the Group Policy Management Console to import the AEM.adm template file into a new or existing GPO, and link the GPO to an AD Organization Unit (OU). With the GPO open for editing, just clicking Enable on the desired GPO setting exposes the customized values, and AEM begins working in the domain. Figure 23.13 displays the actual GPO settings entered during the Enable AEM Wizard step shown in Figure 23.12.

Computers in the OU linked to the GPO will begin sending copies of their error reports to the OpsMgr 2007 server configured to host AEM. Each crash reported by a computer generates an event in OpsMgr 2007. These Application Error events appear in their own section of the Monitoring Workspace in the OpsMgr 2007 console, containing the time of the crash and the involved computer and user names. The event also has event parameters that link to a file containing the Dr. Watson memory dump from the computer with the crash. For enterprises developing their own line of business applications, which is true for many organizations today, AEM can isolate why an application is crashing.

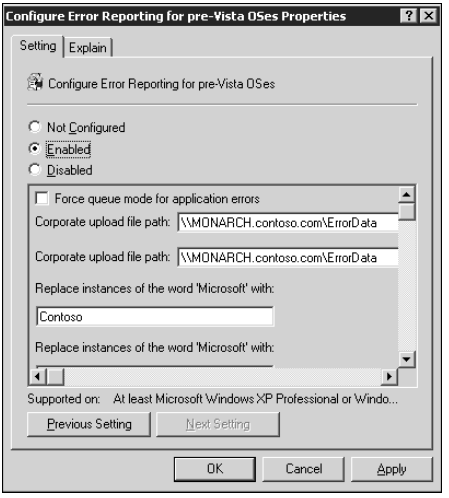


FIGURE 23.13 Client AEM settings reflected in default values of the Group Policy Object settings.

Using Active Directory for Computer Discovery

All versions of Operations Manager including OpsMgr 2007 use a computer discovery process for locating and keeping desired computers in a MOM Management Group. MOM 2005 can effectively discover computers (both manually and automatically) but is not very flexible or necessarily intuitive. The computer discovery process used by MOM 2005 allowed you to search and filter by domain name, computer name, and whether to include domain controllers.

As mentioned in the first section of this chapter, one new way OpsMgr 2007 uses Active Directory (AD) is to preassign computers to management servers so that the OpsMgr agents can be installed with a hard drive image. Launching the Discovery Wizard from the OpsMgr console offers the administrator more AD-integrated options for locating computers to manage.

To make it more intuitive to manage every computer in the domain, there is a new one-click option in OpsMgr 2007 to perform Automatic Computer Discovery. As an extension to MOM 2005's discovery feature set, you can now also create an advanced query using various AD attributes such as Description as well as operating system (OS) attributes such as the OS version.

Figure 23.14 shows the new Discovery Wizard after selecting the option to perform an Advanced Discovery (rather than an Automatic Computer Discovery) and configuring an advanced query to include client computers running the Windows XP operating system.

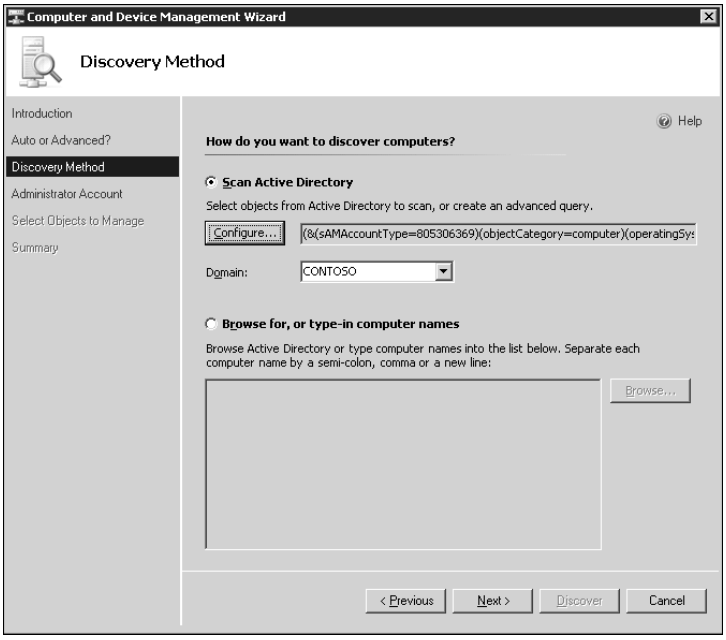


FIGURE 23.14 Using the OpsMgr 2007 Discovery Wizard to discover Windows XP client computers.

Audit Collection System

All Windows computers have three common event logs: System, Application, and Security. The System and Application logs are generally only of interest to network administrators. The Security log, however, can sometimes be the subject of interest by other parties, such as the Human Resources (HR) department, or even the legal department or a court of law. Another distinction the Security log holds is that even with only a few security auditing features enabled the Security log grows and fills up much faster than the other logs. Central collection and retention of Security logs has always been problematic due to the titanic quantity of security events across the enterprise when enabling auditing.

Microsoft is starting to provide network administrators with relief in managing security audit events with the new Audit Collection System (ACS) in OpsMgr 2007. The OpsMgr 2007 Agent includes new technology known as the ACS forwarder. Implementing ACS with OpsMgr 2007 requires installing the ACS server component on an OpsMgr 2007 management server, which cannot be the primary or first management server in the OpsMgr management group. Data is stored in an ACS-created SQL database independent of the OpsMgr databases.

The ACS forwarder component of the OpsMgr Agent locates the ACS server using Domain Name System (DNS) Service Location (SRV) records to locate the "_adtserver" service using port 51909. Audit events are streamed over the network to the ACS server, which writes the events immediately to the ACS database.

Implementation of ACS does not increase the amount of data in the OpsMgr 2007 operational or reporting databases. However, the ACS database integrates with the OpsMgr 2007 Reporting function, enabling the administrator to generate OpsMgr 2007 security audit event reports such as "Who Logged on When and Where."

New Alert Notification Technologies

Spreading the word when there is a problem is a key component in any monitoring solution whether simple or complex. In MOM 2005, some or most alerts often require no notification action other than normal generation of an alert and possible state change event. It is possible to "overnotify" computer operators and administrators to a point where they can miss the most critical events—this is only human nature.

Alerts on some key monitors, however, may be business critical or may require the assistance of a Subject Matter Expert (SME), or the administrator may just be out of the office. In these instances, additional notification features are called to reach outside OpsMgr 2007 to those people who need to know what is happening. For these most critical alerts, there is a requirement to design a way to keep an alerting channel open to administrators not watching the OpsMgr Console.

Alerting Via Enhanced Availability Email

One common way to extend the reach of alerts outside the office is for the management program to send alert notification to administrator(s) via email, typically using Simple Mail Transfer Protocol (SMTP). Using SMTP is convenient but always leaves some uncertainty as to whether the email system is available.

MOM 2005, like many management applications, provides for the entry of only one SMTP server name for use by a MOM management group when sending outbound email notifications. This presents availability issues when that particular SMTP server is down for maintenance or inaccessible due to connectivity issues.

OpsMgr 2007 introduces an enhancement to alert notification via SMTP with the ability to specify additional SMTP servers to deliver outbound notifications. You can specify one primary and multiple, prioritized failover SMTP servers, each using a different authentication method and a user-defined fail-back threshold. This innovation is a welcome relief for increasing the availability of email for notification delivery.

In Figure 23.15, notice how we specify an internal SMTP server, using Windows Authentication, as our Primary SMTP notification server. We also specify a failover SMTP server, in this case an example external mail host, perhaps at an Internet Service Provider (ISP) to bypass the corporate email system.

Alerting Via Instant Messaging with Live Communication Server

Instant Messaging (IM) has evolved into a communications mainstay, and OpsMgr 2007 joins the cause with a new notification feature utilizing Microsoft's corporate IM product, Live Communications Server 2005 (LCS). The primary IM client for LCS is Office Communicator 2005.

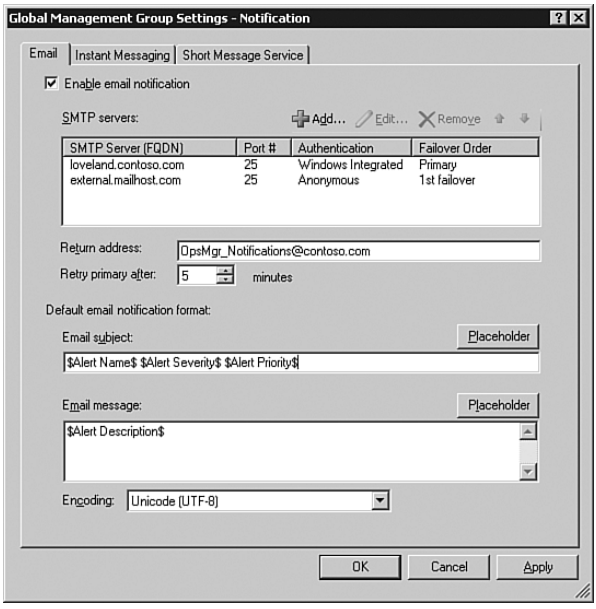


FIGURE 23.15 Specifying multiple outbound SMTP servers adds fault tolerance to deliver OpsMgr 2007 Alert Notifications via email.

We recommend that every medium- to large-sized IT shop evaluate LCS and Office Communicator for use as a corporate IM system. With a proper LCS deployment, enterprises benefit from a locked-down, advertisement-free way for employees to communicate rapidly and efficiently. Ideally, corporate IT users run only Office Communicator on their desktops, with direct connection to commercial Internet-based IM services restricted at the firewall.

Comprehensive IM encryption, archiving IMs, and even some IM content control is built into LCS. The LCS architecture includes an LCS Access Proxy application that permits users to participate in the corporate IM system over the Internet as well.

Microsoft provides an LCS external connector to commercial IM networks such as Yahoo!, MSN, and AOL for selected corporate IM users such as IT administrators. Office Communicator 2005 also has great mobile appeal, with web-based and Windows Mobile versions.

The OpsMgr 2007 administrator can easily architect a broad-reaching notification solution using OpsMgr 2007, LCS, and Office Communicator. In Figure 23.16, we configure OpsMgr 2007 to use the Transport Layer Security (TLS) protocol to communicate with the LCS IM server over the default TLS port 5061. TLS is the most secure way to implement LCS because it provides end-to-end encryption of instant messages.

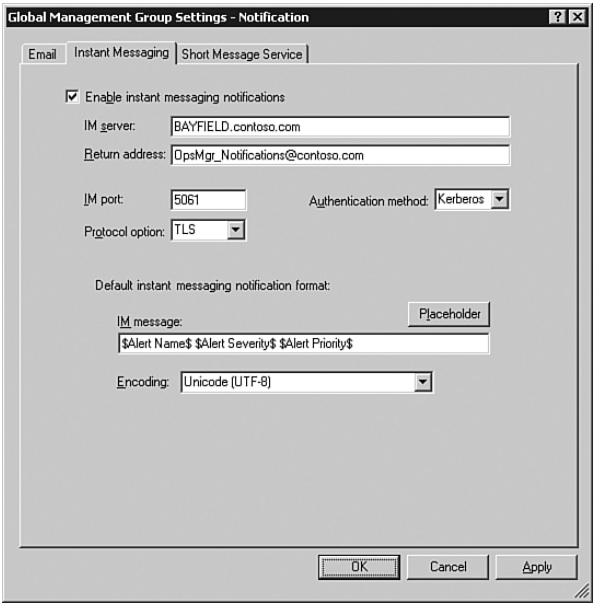


FIGURE 23.16 Configuring OpsMgr 2007 to securely transmit Alert Notifications using Instant Messaging.

Network Device Monitoring

A well-known "feature" in MOM 2005 is that "everything is a computer." As we discussed in Chapter 20, "Developing Management Packs," the MOM 2005 architecture allows administrators to manually add non-Windows devices to the list of managed computers, although MOM 2005 treats each device as a computer anyway. Devices such as routers and switches, even with the Simple Network Management Protocol (SNMP) enabled, appear as Unmanaged Computers in the MOM 2005 consoles.

Operations Manager 2007 adds new built-in support for managing SNMP-enabled devices, such as routers, print servers, and non–Windows-based systems. OpsMgr 2007 can obtain a core set of data from SNMP-enabled devices and non–Windows-based computers, using the MIB-II standard set of identification data and utilization statistics. MIB-II (Management Information Base, generation two) is the globally accepted standard set of SNMP properties needed to manage a network object using TCP/IP. OpsMgr 2007 queries network devices for MIB-II values and displays them in the OpsMgr console.

New Discovery Method for Network Devices

The "Using Active Directory for Computer Discovery" section earlier in this chapter previews some of the new AD integration features in the discovery process using the Advanced Discovery option in the Discovery Wizard. Another selection available with the Advanced Discovery option is to discover network devices.

The new network device discovery process for OpsMgr 2007 is simple—you give the Discovery Wizard a start and end address for the search and a SMTP community string such as the common read-only SNMP community string "public." After the search is completed, the administrator is given a list of discovered active SNMP devices. Selected devices are brought into OpsMgr 2007 management as network devices.

Monitoring Non-Windows Platforms

After the wizard discovers network devices and you select which ones to manage, you can view their state in the Network Devices section of the OpsMgr 2007 Monitoring Workspace. Figure 23.17 shows seven monitored network devices: four Cisco switches, a Cisco router, an HP ProCurve switch, and an HP JetDirect print server. The Device Description column is populated using data obtained via SNMP from the MIB-II.

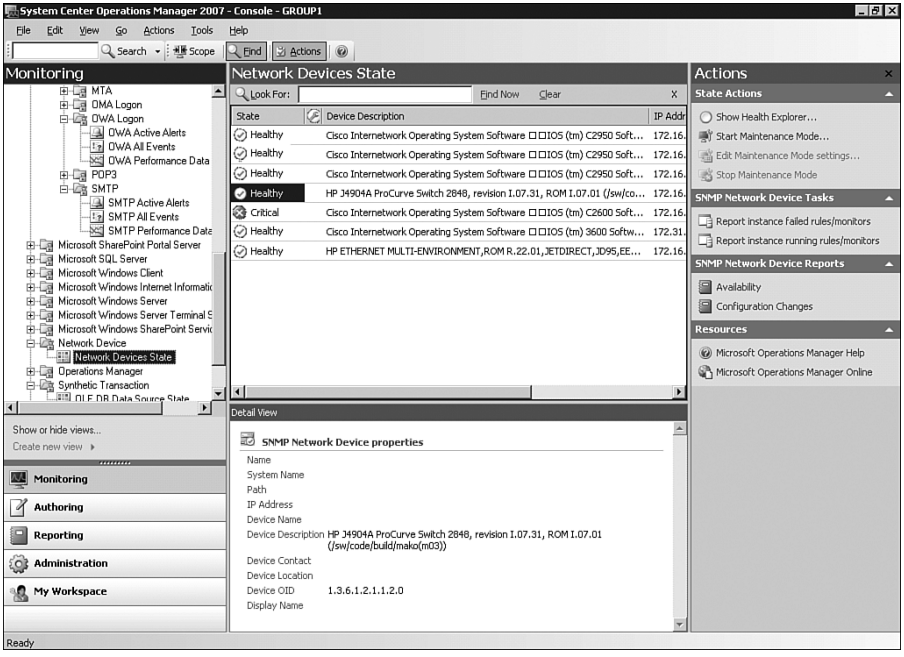


FIGURE 23.17 Using OpsMgr 2007 to monitor the state of network devices such as switches and routers.

Migrating to Service-Oriented Monitoring

In the "Moving Toward Application-Centered Management" section earlier in this chapter, we suggested that in the near future network administrators would seek application- (or service-) oriented SLAs. When Internet-based applications are competitive with computer and server-based applications in price, performance, availability, and security, decision-makers may not care how applications are delivered to users. An SLA based on

the performance of a given number of application servers is less useful than one based on the application itself being available and responding correctly as needed.

The savvy Technical Decision Maker of the future is empowering a new dynamic in the IT industry—monitoring distributed service and application delivery systems. The health of these systems will be assessed by the performance and availability of those applications to their users. SLAs deliberately avoid limiting the nature of application delivery, allowing the service provider the flexibility to change out pieces of the system while the service is provided.

In a world of delivered software, there is a need for a "quality assurance monitor" at the point of consumption to verify its delivery. Microsoft lets us build those application delivery quality monitors today with new OpsMgr 2007 technologies. These utilities operate at the user level and even in the user location, observing application delivery quality for expected or desired results.

We will discuss several ways of creating monitors to capture and assess application end-user experience based on templates built into OpsMgr 2007. Inventing and adapting these user-experience monitors, which function like probes, takes place in the Authoring Workspace of the OpsMgr 2007 console. Let's look at the Authoring Workspace Overview in Figure 23.18. We can run the Add Monitoring Wizard from the Authoring Workspace to demonstrate the new Synthetic Transactions and Web Application monitoring features.

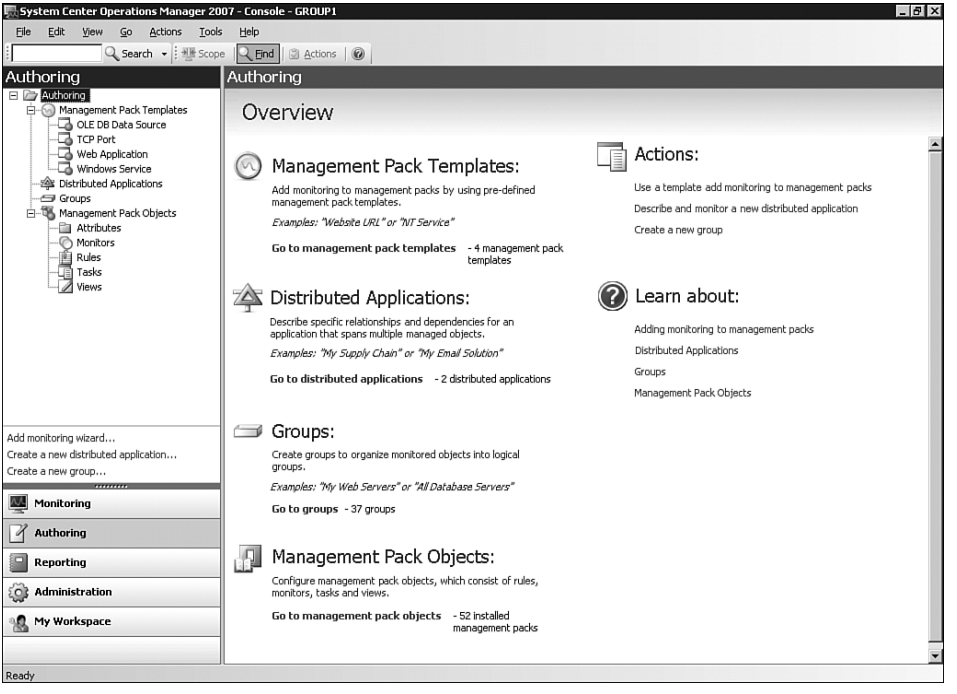


FIGURE 23.18 OpsMgr 2007 Authoring Workspace: Where most customization work in OpsMgr 2007 occurs.

Using Synthetic Transactions

Launching the Add Monitoring Wizard from the OpsMgr 2007 console's Authoring Workspace steps you through the process of creating a management pack using one of several supplied Management Pack Templates. The templates you can select are listed near the top of the workspace, in the upper left of Figure 23.18. Two of these Management Pack Templates, OLE DB Data Source and TCP Port, create monitored objects in the Synthetic Transaction section of the Monitoring Workspace.

- The OLE DB Data Source template allows you to monitor an OLE DB source. You can choose from a list of OLE DB providers or supply a connection string to monitor the target data source. The list of available OLE DB providers includes ODBC Drivers, Microsoft Jet, SQL Native Client, Oracle, and others.
- The TCP Port template allows you to create a monitor for an application listening on a specific TCP or User Datagram Protocol (UDP) port. You can enter the IP address and port to monitor, such as a well-known application port like SMTP (TCP port 25) or DNS (UDP port 53), or a custom application on a port you specify.

To realistically monitor service delivery, you need to actually locate your monitors where the service is delivered. OpsMgr 2007 makes this easy because the Add Monitoring Wizard has you choose the managed computer(s) that will monitor the synthetic transaction. These managed computers are called *watcher nodes* in OpsMgr 2007. Each custom Synthetic Transaction you create is executed from the chosen watcher nodes.

Although the state of all synthetic transactions you create is viewable in the Synthetic Transaction section of the Monitoring Workspace, the real reason for creating synthetic transactions is to use them as building blocks in a larger, more comprehensive distributed application that is the actual monitored object of interest. We will describe how to do that shortly in the "Distributed Applications" section of this chapter.

Monitoring Web Applications

While running the Add Monitoring Wizard, selecting the Web Application template opens the door to a completely new, full-featured studio of authoring tools. These tools can be used to assemble a multicomponent simulator of the desired user experience. We set up an example web application for our scenario: A PC at a branch office accesses a Line of Business (LOB) application over the corporate intranet, enters text on a web page, and receives a certain response in a timely manner.

In this instance, we created a Web Application Monitor that tests for the successful use of application "X" from a computer at site "Y" when launched from the corporate intranet page. In this example, the watcher node computer WINTERPARK is a PC located at Site "Y." Figure 23.19 shows the summary of our web application monitor settings.

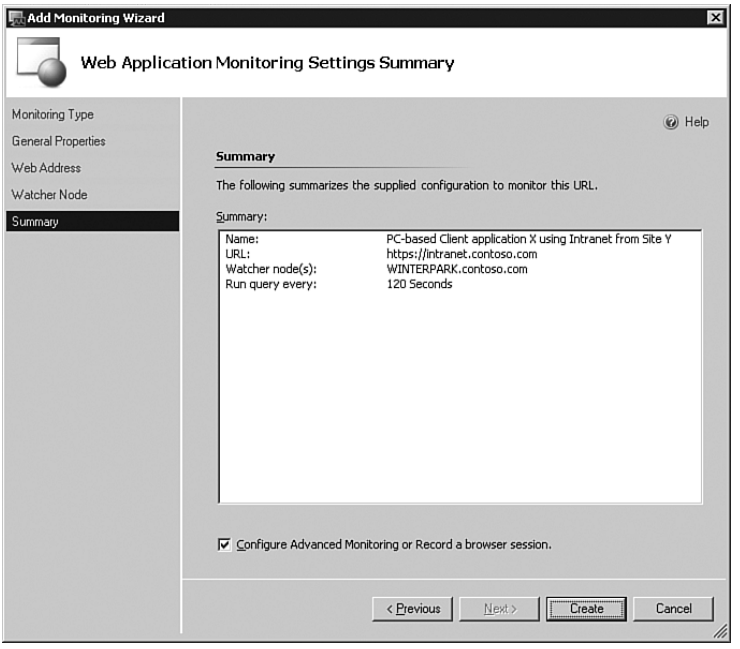


FIGURE 23.19 Web Application Monitoring Settings Summary; intranet availability viewed by a watcher node.

The Web Application Monitoring Settings Summary displays in the console after running the Add Monitoring Wizard and furnishing the basic information to create a web page monitor. Notice the option we selected at the bottom of the summary—Configure Advanced Monitoring or Record a Browser Session:

- When this option is *not* selected, clicking the Create button produces a simple Uniform Resource Locator (URL) monitor that alerts if anything other than response code 200, indicating a successful URL retrieval, is encountered.
- Checking Configure Advanced Monitoring and selecting Create opens the Web Application Editor displayed in Figure 23.20.

We can use the Web Application Editor to add functionality to the simple "web page" monitor, upgrading it to a sophisticated "web application" monitor. The top center portion of the Web Application Editor lists the websites the monitor will examine. When you first open the Web Application Editor after creating the basic web application monitor, only the first URL request is listed in the top section of the Editor—in this case https://intranet.contoso.com.

Let's say not only do we want to monitor that the computer can open the corporate intranet, but we also want to make sure that the computer can get to the Microsoft Search site using the URL http://www.microsoft.com/search. (Perhaps this system is a tech support workstation that needs to access the Microsoft search engine for help desk staff to do their jobs.) We use the Group Requests action in the Editor to put the first URL request in a descriptive request group labeled Open Browser to Contoso Intranet.

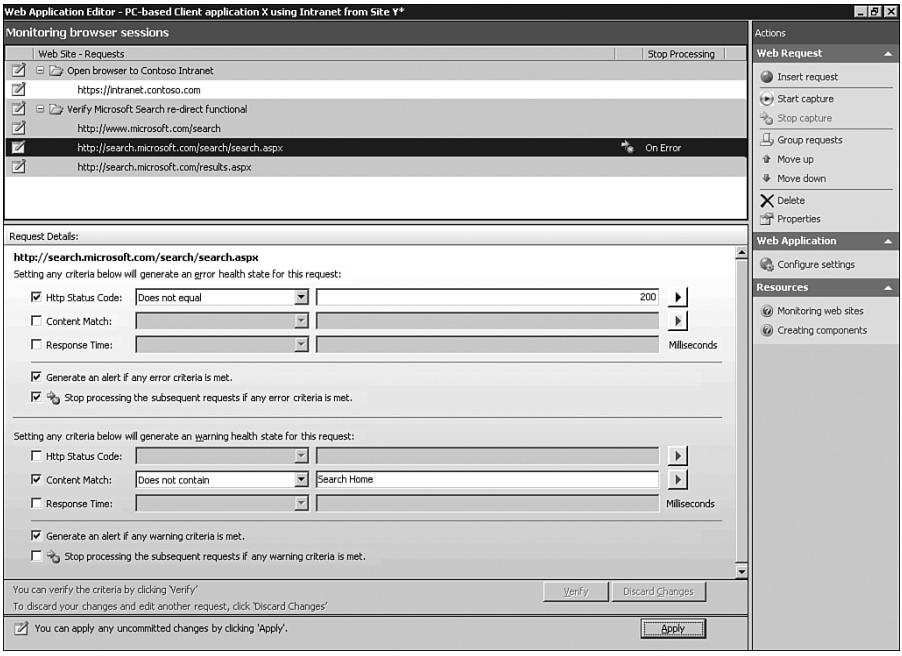


FIGURE 23.20 The OpsMgr 2007 Web Application Monitoring Editor is a full-featured authoring environment.

Now use the Start Capture action in the Editor to open a new OpsMgr 2007 web browser session recorder. The web session recorder looks like a panel down the left side of the browser, with record/pause/stop controls in a toolbar. With our session recorder running, when we browse to Microsoft's search engine we are redirected from http://www.microsoft.com/search to a page at http://search.microsoft.com.

When we complete our web session capture and return to the Web Application Editor, the captured URLs we visited in our browser are listed in the Web Site Requests section. We can create a new request group using the descriptive name Verify Microsoft Search Re-direct Functional and move the captured URLs at microsoft.com to that group.

In Figure 23.20, the highlighted URL at search.microsoft.com has secondary alert criteria specified in the lower central portion of the Web Application Editor. As shown in the Request Details section, an error state (actually displayed in red) exists when the HTTP Status Code is not the expected and normal 200. If the HTTP Status Code is 200, request processing continues, and a warning state (displayed in yellow) exists if the words "Search Home" are not found on the page. (The actual Microsoft Search page at the redirected site contains the words "Search Home.") This second check verifies not only that the redirection is taking place but also that users are able to access the correct web page.

As a final step, we can add custom monitor error criteria to our http://search.microsoft.com website request. The monitor examines custom criteria after it performs the primary checks specified in the Request Details area in Figure 23.20. In our example we want to make sure not only that users can get to the correct page at search.microsoft.com but also

that there are no delays in some key measurements of application responsiveness. In other words, we want to measure the website's usability. You can select the Configure Settings action in the Editor to bring up a multitabbed Request Properties box, displayed in Figure 23.21.

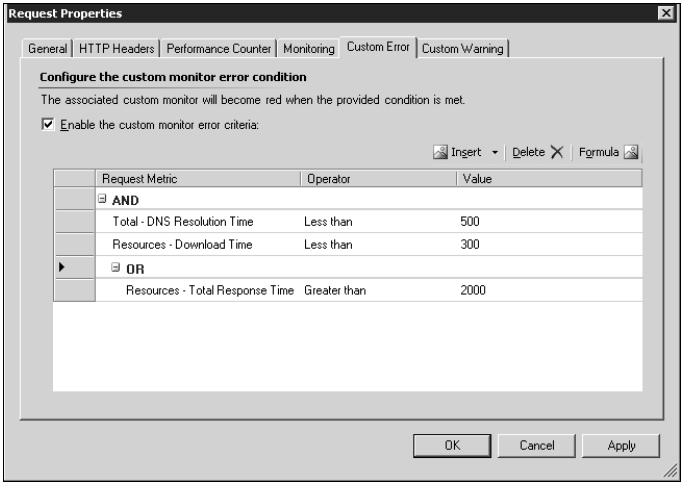


FIGURE 23.21 Using the Web Application Monitoring Editor to configure custom monitor error conditions.

The simple language on the Custom Error tab of the Request Properties box in Figure 23.21 explains the effect of setting these custom criteria: "The associated custom monitor will become red when the provided condition is met." Notice in Figure 23.21 that we were able to use AND / OR branching when building the custom criteria. This is a powerful feature when it comes to application performance monitoring!

In our Web Application Monitoring scenario, we selected six discrete events to monitor. We can check these conditions using the Client Application X Using Intranet from Site Y web application monitor, using the perspective of the PC selected in site "Y" as our watcher node:

1. The corporate intranet is available at URL https://intranet.contoso.com.
2. The URL http://www.microsoft.com/search is available as is the redirect to the URL http://search.microsoft.com.
3. The page returned from http://search.microsoft.com is checked for the words "Search Home."
4. The DNS resolution time is verified to be less than 0.5 seconds; AND

5. The Resource Download Time is less than 0.3 seconds (intranet support is not slow).
6. The Total Resource Response Time is not greater than 2 seconds. (Application is not running slowly.)

Now we have a specific, targeted Web Application monitor that represents a critical business process where Help Desk employees perform their work at a branch location. Next we will use the custom Web Application monitor as a building block in creating a Distributed Application monitor.

Distributed Applications

We now move to the crown jewel of the new capabilities in OpsMgr 2007—the Distributed Application Designer. In the "Network Device Monitoring" section earlier in this chapter, we describe how OpsMgr 2007 manages *objects* rather than *computers*. In OpsMgr 2007, computers are now objects, as are network devices, synthetic transactions, custom monitors, and other entities. The Distributed Application Designer is where we author a view of our application or service composed of any variety of physical and logical objects in our management group.

Using the Distributed Application Designer, we can easily pick and choose those objects from among those provided by OpsMgr 2007 management packs, as well as any created for our custom applications and requirements. Administrators using OpsMgr 2007 to monitor distributed applications will repeat this process using the following steps:

1. Install Microsoft and vendor-supplied OpsMgr 2007 management packs.
2. Discover computers and network devices.
3. Confirm basic monitoring is occurring as desired and collect baseline profiles.
4. Author custom objects such as synthetic transactions and Web Application monitors to capture unique Line of Business aspects.
5. Design Distributed Application monitors using objects to create components, and define relationships between the components.
6. Focus on managing the distributed applications.

Our sample distributed monitoring application, the Contoso Intranet Help Desk Application, highlights these concepts. We include custom objects created earlier in the "Using Synthetic Transactions" and "Monitoring Web Applications" sections of this chapter, as well as network devices and other objects, to create an intelligent map of our application's health.

We begin the process by running the Create a New Distributed Application Wizard from the Authoring Workspace. After naming the application and selecting a Distributed Application template, the wizard closes, and the Distributed Application Designer opens displaying the initial view, shown in Figure 23.22.

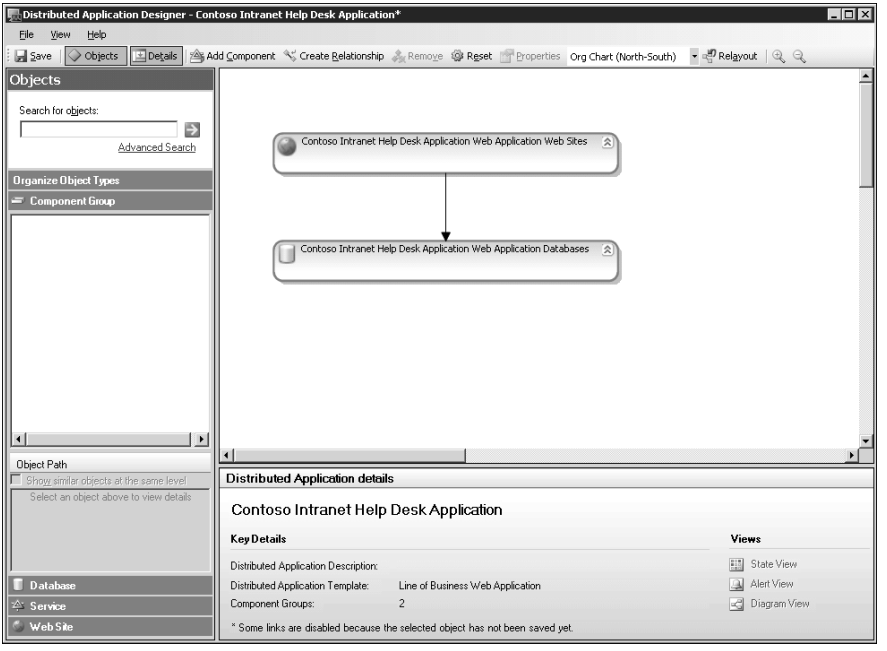


FIGURE 23.22 Initial view of Distributed Application Designer when creating a Line of Business Web Application.

Selecting the Line of Business Web Application template in the Create a New Distributed Application Wizard causes the wizard to create the initial application view (displayed in Figure 23.22) of two components and a defined relationship. The initial distributed application has these elements: a component of one or more websites, dependent on a component of one or more database servers. This is a logical generic depiction of a distributed web application and really gives us a head start towards creating our application.

Now we flesh out the web application from the template with meaningful objects we select. We can add any object in the OpsMgr group to our application map:

1. To the premade websites and database server components, we add server health monitors for the web and database servers, as well as targeted performance counters such as CPU for the database server and Internet Information Services (IIS) for the web server. We add a custom Service Monitor for virus scanning software on the web services component.

2. Next, we create new components such as Datacenter routers and Datacenter switches, and add appropriate managed network devices to those components.

3. We also create a component to hold objects that represent the health of branch office "Y," and add the custom synthetic transaction and web application monitoring objects previously created. We can click, drag, and resize our components easily.

4. Finally, we select the Create Relationship tool and click from component to component to create a component dependency hierarchy.

Figure 23.23 shows the completed example Distributed Application object.

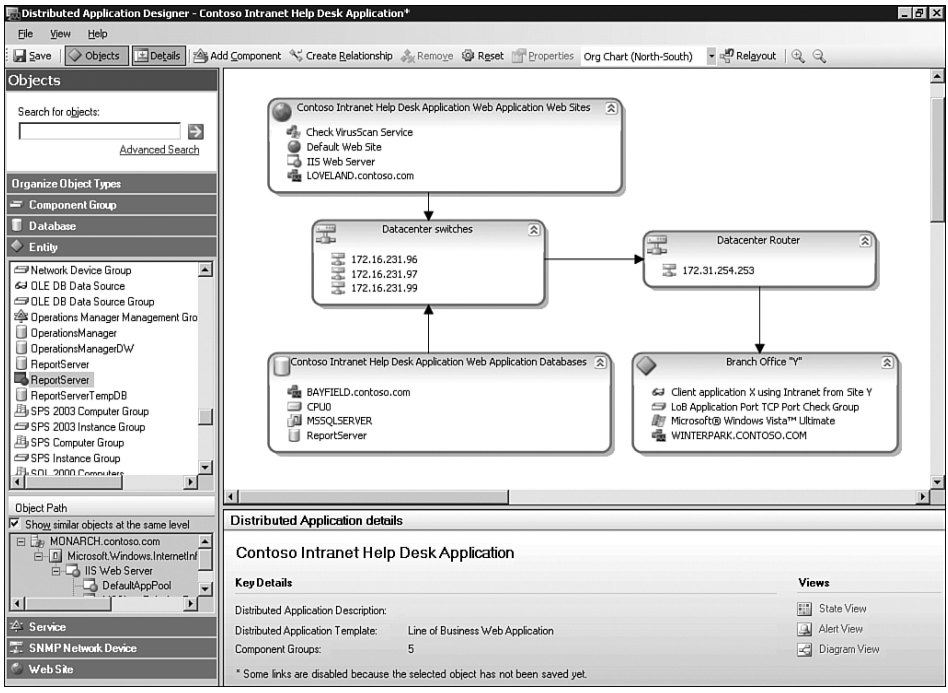


FIGURE 23.23 Line of Business web application created in the Distributed Application Designer.

After saving our Distributed Application, the overall state of the application can be seen in the Global Views section in the OpsMgr 2007 Monitoring Workspace—a prime location in the console. If the application has a problem, the idea is to select the Diagram view as a first step towards problem resolution. The Diagram view is an application topology map generated and updated by the OpsMgr console.

The console renders the Diagram view based on the component relationships we defined when we authored the application. The virtualization of an application using objects, components, and component relationships, with health state of the objects determined by certain criteria, is sometimes referred to as its *health model*.

The administrator can review the live monitoring state indicators on the topology map to instantly spot failure points. Figure 23.24 displays the real-time monitoring Diagram view for the Contoso Intranet Help Desk Application we created in this chapter. Notice the Overview tool floating in the upper-right part of the diagram. This is a useful navigation tool for "flying around" in a larger map, as well as zooming the scale of the map.

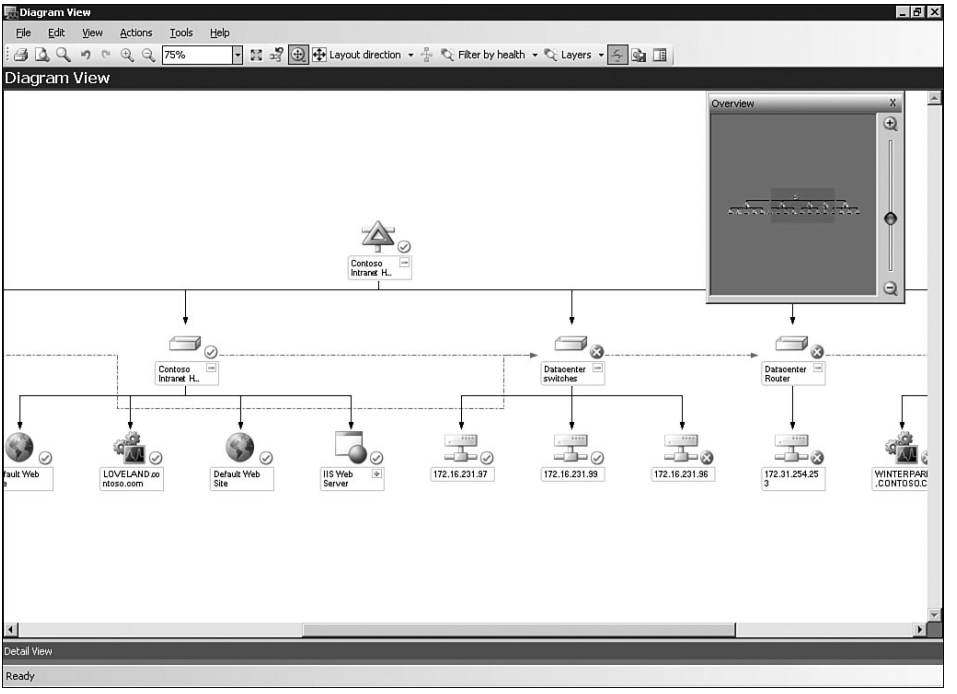


FIGURE 23.24 Live multiplatform event correlation using the Diagram view of a distributed application.

Changes to Security Architecture

OpsMgr 2007 administrators must belong to a single domain Global or Universal security group specified during the installation process. This group does not have to be the Windows Administrators group, and the selected group can be changed after installation. As was the case in MOM 2005, a trust relationship between domains is not required for OpsMgr 2007 in one domain to manage computers in another domain. Also similar to MOM 2005, OpsMgr 2007 includes the concept of an Action account.

The primary new security-related feature of OpsMgr 2007 is user roles. User roles are a welcome addition to OpsMgr because MOM 2005 had limited support for this concept. MOM 2005 security could be manually manipulated using AD security and MOM 2005 Console Scopes, but this was a tedious process and not one MOM 2005 was designed for. With proper role-based security, a particular user will see a compartmentalized view of only those objects, tasks, and tools appropriate for his function—no more and no less.

Operations Manager 2007 includes more than 150 operations such as resolving alerts, executing tasks, overriding monitors, creating user roles, and viewing alerts. These OpsMgr-specific operations are grouped into *profiles*, each profile representing a particular job function. Job functions include Read-only Operator, Advanced Operator, Author, Administrator, and a few others.

A *scope* defines the entity groups and classes the profile is restricted to. For example, a scope might include computers in a particular domain and exclude computers from all other domains. A scope also specifies the tasks and views granted for each type of managed object. User roles are the combination of a profile and scope. User roles allow a user to be assigned a role tailored to her job function and "need to know." These assignments are made in the OpsMgr 2007 console's Administration Workspace.

Changes to Management Pack Architecture

Management packs in MOM 2005 function as container and distribution vehicles used to deploy configuration information required for managing computers and applications. MOM 2005 MPs consist of collections of rules, knowledge, and public views, determining how a MOM management server collects, handles, and responds to data. MOM 2005 MPs expect all discovered objects to be computers, making the management packs lists of functionalities that manage specific computers and computer groups.

Management packs for Operations Manager 2007 focus on discovering and monitoring applications, components, and devices, referred to collectively in OpsMgr 2007 as *objects*. Discovered objects are monitored based on their health models, defined in the respective OpsMgr 2007 management pack. OpsMgr 2007 MPs can define any object or combination of objects as management entities, giving us an infinite assortment of possible functionalities.

Management packs in MOM 2005 are distributed and exported as one type, a binary file type with the .AKM file extension. The author of an MP in MOM 2005 can specify that the Knowledge is read-only. However, nothing prevents a MOM 2005 administrator from modifying the rules created in MOM 2005 after importing an MP. Keeping track of those customized and modified rules—their location, names, and other logistical matters—can become a management burden in large environments.

OpsMgr 2007 makes it easier to "manage the management packs" by introducing the concept of a sealed management pack with the .MP file extension. Sealed MPs cannot be modified and are read-only in OpsMgr 2007. The MP format is a binary format, like the MOM 2005 .AKM format; however, OpsMgr 2007 MP files and MOM 2005 AKM files are not interoperable.

OpsMgr 2007 modifies MP behavior using rule and criteria overrides similar to that of MOM 2005. The override process modifies how a rule functions regarding a particular object. What changes with this new version is how it handles new and modified rules:

- In MOM 2005, new rules and rule modifications can be saved within any rule group, resulting in co-mingled vendor-supplied and user-created or user-modified rules.
- OpsMgr 2007 requires that new and modified rules are saved to their own separate (unsealed) management packs.

The only supported file operations for sealed .MP files are import and uninstall. MPs function like add-ins in other Microsoft applications and are created by hardware and software manufacturers and vendors. These MPs are sealed by digital certificates, in a manner similar to the signing of Windows hardware drivers. The vendor's certificate provides positive identification and validation of the MP's authenticity.

OpsMgr 2007 also introduces a second new type of management pack, the .XML format MP, which is an editable file with the .XML file extension. XML management packs can be edited using authoring tools in the OpsMgr 2007 console.

Migrating Management Packs

In the OpsMgr 2007 beta, MOM 2005 management packs are converted to OpsMgr 2007 management packs using a two-step process. First, the MP2XML utility converts the MOM 2005 MP from .AKM file format to MOM 2005 .XML file format. The MOM 2005 .XML file is then converted to OpsMgr 2007 .XML file format with the MPConvert support tool.

System Center Essentials 2007

In the "Microsoft System Center Evolution" section earlier in this chapter, we mentioned the Service Center Essentials member of the System Center (SC) family. Microsoft positions System Center Essentials as its new health monitoring and change-and-configuration management solution for the small- to medium-sized organization.

Introducing System Center Essentials

SC Essentials 2007 is a beta application that accomplishes health monitoring and change-and-configuration management by combining the monitoring features of SC OpsMgr with the inventory and software distribution functions of SC Configuration Manager. The monitoring function takes the form of a simplified OpsMgr 2007 engine, and the software distribution function is performed by the WSUS version 3.0 engine. SCE is a wrap-around shell and user interface for these functionalities on a small business network.

SCE is expected to be available as a standalone product, and it is also believed that Microsoft will bundle SCE 2007 with the Windows Server "Longhorn" version of Small Business Server, code-named "Centro." Using SCE, you can centrally manage Microsoft Windows-based servers and PCs, as well as network devices, by performing the following tasks:

- Monitor the health of computers and network devices and view summary reports of computer health.
- Centrally distribute software updates, track installation progress, and troubleshoot problems by using the update management feature.
- Centrally deploy software, track progress, and troubleshoot problems by using the software deployment feature.

- Collect and examine computer hardware and software inventory by using the inventory feature.

Differences Between SCE and OpsMgr 2007

SCE provides a small subset of OpsMgr 2007 functionality when it comes to monitoring and managing infrastructures. The flip side of this reduced functionality is that SCE greatly simplifies many functions compared to its OpsMgr 2007 counterparts. For example, by default the Discovery Wizard in SCE automatically searches for both Windows computers and SNMP-based network devices in the SCE server's domain and local subnet without requiring the user to enter any networking information.

Customization and connectivity options for SCE are limited, however. A SCE deployment will always consist of a single server, the SCE server that runs all the monitoring and software management components, including two SQL Server 2005 Express databases.

In addition to the functionality differences, SCE limits the number of managed objects per deployment to 30 Windows server-based computers, 500 Windows non–server-based computers, and a yet unknown number of network devices. (Microsoft has not yet decided the upper limit on network devices.)

Solutions for Service Providers

System Center Essentials 2007 also offers a mode of operation that is intriguing for businesses in the Managed Service Provider (MSP) industry. A *MSP* is a technology services company that partners with an organization to manage some or all of that organization's IT services, usually remotely over the Internet. MSPs typically deliver infrastructure management services on a subscription basis, similar to the model used by Application Service Providers (ASPs).

Most network management applications are created for use by the medium to large network administrator, including MOM 2005 and OpsMgr 2007. These enterprise applications are necessarily a bit bulky and complex to scale to manage possibly thousands of devices in many physical locations. The administrators of small to medium networks have generally not been able to leverage the enterprise management products.

Microsoft is engineering a way to connect a SCE server running on a small business network to an OpsMgr 2007 management group in an MSP's Network Operations Center (NOC). When OpsMgr 2007 and SCE 2007 are coupled together this way, it is known as the *Value Added Provider (VAP) Scenario*. Think of an OpsMgr "mother ship," connecting to many "satellite" SCE nodes using SSL channels over the Internet. When SCE operates in the VAP Scenario, the SCE server in essence becomes a watcher node of the MSP's OpsMgr group, extending the scope of the MSP's OpsMgr group to include all the computers and network devices on the connected small business networks.

SCE on the small business network functions as a probe for OpsMgr 2007, forwarding alerts to the OpsMgr group. The small network administrator is then able to leverage the enterprise management software, facilities, staff, and knowledge of the MSP. The MSP can

charge a profitable subscription service fee, which is still a bargain for the small business administrator, who gets possibly 24x7 "eyes on" monitoring at a fraction of the cost it would take to establish an effective monitoring regimen without SCE and an MSP.

Migration Scenarios

As we mentioned in the "Transitioning from a Microsoft Operations Manager 2005 Ecosystem" section earlier in this chapter, if you are interested in using OpsMgr 2007 the best approach is to install MOM 2005 and begin collecting data. If you use MOM 2005, you will want to evaluate and test the new version of Operations Manager.

A MOM 2005 environment can convert to OpsMgr 2007 with the same hardware that the MOM 2005 server components are using or upgrade to new server hardware running OpsMgr 2007. There are three supported migration scenarios for moving from MOM 2005 SP1 to OpsMgr 2007. MOM 2005 customers might make use of the following information in planning server life cycle management.

- Same hardware approach—All OpsMgr 2007 components, including databases, management servers, consoles, and agents, are installed on systems running the corresponding MOM 2005 versions. In this scenario, you have full functionality of both MOM 2005 and OpsMgr 2007 (but no communication between the versions). Start to retire the MOM 2005 environment when you are satisfied that OpsMgr 2007 is reliably doing the monitoring job.
- Side-by-side conversion—In this scenario, customized MOM 2005 MPs are exported and converted to OpsMgr 2007 format. It is necessary to preserve only custom management packs. Uninstall MOM 2005, install OpsMgr 2007, and import the custom MPs. This scenario runs OpsMgr 2007 on the same hardware as MOM 2005 but necessitates a period without monitoring services during the conversion.
- New hardware approach—This is a conventional approach that installs OpsMgr 2007 server components on new hardware. When the OpsMgr 2007 agents are installed, they effectively dual-home the managed computers and report into both the 2005 and 2007 Operations Manager management groups. The MOM 2005 and OpsMgr 2007 environments run independently. You can migrate monitoring responsibility to OpsMgr 2007 at a comfortable pace.

Summary

Microsoft looks to have made some wise decisions surrounding the development and architecture of System Center. This introductory tour of a beta version of Operations Manager 2007 has shown that the new version of OpsMgr is much more than a set of feature upgrades to MOM 2005. We have learned how OpsMgr 2007 fits into an all-new family of System Center applications, and we saw how OpsMgr 2007 presents a wealth of meaningful and useful information in its new single console, which includes sophisticated authoring tools. We also gained awareness of a new paradigm of assessing application health based on synthetic transactions and distributed application monitoring tools.

PART VII
Appendixes

IN THIS PART

This page intentionally left blank

APPENDIX A

MOM Internals

IN THIS APPENDIX

We now peek under the covers to examine some internal workings of Microsoft Operations Manager (MOM) 2005. We examine files used by the management server and a managed client. We also discuss event and runtime processing and the heartbeat process, which is a key piece of agent functionality.

Directory Structure

MOM utilizes temporary or queue files for transient processing. These queue files are found both on the agent and the server. The management server provides agent management capabilities for itself and agentless-managed servers; it also utilizes agent queue files in addition to the management server queue structure. We describe these files and files used for logging.

Queue Files

Queue files used are stored on the managed agent and the management server at *%ALLUSERSPROFILE%*\Application Data\Microsoft\Microsoft Operations Manager\ <*management group name*>. Significant files include

- AgentQueue.pqf—Agent queue file.
- AgentQueue.wkf—Workfile.
- ConfigCache—Includes rules, scripts, providers, and configuration information provided by the MOM Server component.

More about ConfigCache

The ConfigCache is updated by the Configuration Manager as described in the "Configuration Flow of the MOM Server" section later in this appendix.

- EventCons—Includes consolidated events.
- EventCons.wkf—Workfile.
- EvtSend.pdf—Agent temporary storage (events).
- AlertSend.pdf—Agent temporary storage (alerts).

In addition to the files in the preceding list, the following queue files are located on the management server only:

- ServerCache—Server Cache.
- ServerQueue.pqf—Server Queue file.
- ServerQueue.wkf—Workfile.

Do Not Scan the Queue Files for Viruses

Antivirus real-time scanning of the queue files is not recommended; it will cause serious problems with response time.

The queue files cannot be opened to view their contents (such as the types of events being processed, for example). By default, the maximum size for the any individual queue on the management server is 30000 Kilobytes (KB) (30 Megabytes [MB]). You can increase this setting to as high as 90000KB (90MB); verify that there will be sufficient size in that disk partition to accommodate the larger files. The default queue size for agents is 3000KB (3MB). Queue files end with a .pqf extension, and the file size maximum applies to these files only; .wkf files are not included in the limit.

The agent queue file setting is maintained in the MOM 2005 Administrator console under Administration \ Global Settings \ Agents \ Temporary Storage tab. To modify the queue file settings for the management server, edit the management server's properties under Administration \ Computers \ Management Servers. Right-click on the targeted management server; then select Properties. Now click on the Temporary Storage tab and uncheck Use Global Settings. You can now change both the maximum disk space for temporary storage for the management server and the maximum amount of space used for storing data collected by the agent on the management server.

Caveat About Increasing Queue File Sizes

There actually is no advantage to increasing the temporary storage size unless you are consistently running out of queue space. Significant increases in queue size can actually result in slower processing times!

The queue files can be deleted if you suspect they have been corrupted. If the MOM service has an exception at startup, one troubleshooting approach is to stop the service, delete the queue files, and restart the MOM service, although this does cause the contents

of the queue files to be lost. You can also use the MOMInfo utility (MOMInfo.exe) in the MOM 2005 Resource Kit to clear the queues as documented in knowledge base article 904746 at http://support.microsoft.com/kb/904746/.

Consequences of Deleting the Queue Files

Deleting the queue files will result in a loss of operational data and potentially could result in your SLA (Service Level Agreements) being lowered from lack of supporting data.

Log Files

In addition to the logs typically provided with Microsoft Windows Installer-based installations, MOM 2005 can provide extensive logging for troubleshooting situations. These logs may exist in one of several locations, and each log provides specific data relevant to a process, service, or task.

Enabling Logging

Logging in MOM 2005 is configured in the registry on the target computer by setting the TraceLevel value located at HKEY_LOCAL_MACHINE(HKLM)\SOFTWARE\Mission Critical Software\TraceLevel. A value of 0 will set minimal logging, and a value of 9 enables full, detailed logging. The default value is 1. Setting this value to 0xFFFFFFFF disables logging of all MOM components. This change requires restarting the MOM service.

Logging Levels

A logging level of 6 or below is sufficient for most troubleshooting scenarios. It is advisable to not set the level higher than 6 because this may affect performance of the MOM components. It is best to keep the logging level at the default value (1) when not troubleshooting.

Logging Settings

You can apply several configuration settings to the log files. The following REG_DWORD entries under the HKLM\SOFTWARE\Mission Critical Software registry subkey are relevant to MOM logging:

- TraceInitSeconds—This value specifies the number of seconds to capture startup logging when the MOM service is started. The default value is 0x3c (60 seconds) and controls the length of time that data is written to momservice.mc8, which is then renamed to x(init).mc8.
- TraceCircularLines—This value specifies the number of lines to keep in an iteration of the file. The default value is 0xc350 (50000 decimal). As a log file reaches its maximum size, the current log file is renamed. For example, when the MOMService(B).mc8 log file reaches the value specified in the TraceCircularLines, it is renamed to MOMService(A).mc8 and a new MOMService(B).mc8 log file is

created. When the MOM service is started, the current MOMService(B) and (A) files are renamed to MOMService(B)(1).mc8 and MOMService(A)1.mc8. The four most recent versions of these files are available in the %*windir*%\temp\Microsoft Operations Manager\ folder.

DLLHOST Logging

DLLHost logging is used to troubleshoot issues with the Data Access Service (DAS) and/or the Operator console. To enable DLLHost logging, follow these steps:

1. Change HKLM\SOFTWARE\Mission Critical Software\DASServer\LoggingFlags to FFFF.
2. Change HKLM\SOFTWARE\Mission Critical Software\TraceLevel to 9.
3. Restart the MOM service.

The location of the DLLHOST log file varies depending on whether the activity is DAS-related or whether console activity is being logged:

- DAS activity is stored at *%windir%*\Temp\Microsoft Operations Manager\ dllhost.mc8.
- Operator console activity is logged at *%USERPROFILE%*\local settings\temp\ Microsoft Operations Manager\dllhost(b).mc8.

Script Logging

Scripts can be executed on the server or on the agent. Script logging captures the specific steps as they are performed by a script. To enable script execution logging, first identify which system to log activity for and then perform the following procedure:

1. Modify the registry on the target machine at HKLM\SOFTWARE\Mission Critical Software\Onepoint\EnableActiveDebugging. Change the value from 0 to 1.
2. Restart the MOM service.

The information will be logged to *%windir%*\Temp\Microsoft Operations Manager\ AgentResponses-<*management group name*>.log. Note that if you do not have a script debugger installed you will receive the following warning event in the Application event log:

```
Script Debugger is not installed, hence could not enable active debugging.  Please
install a script debugger.

Provider Name:  Application
Event Number:  9131
Provider Type:  Event Log
Source:  Microsoft Operations Manager
```

File Locations

Log files in MOM 2005 may reside in multiple locations. Table A.1 lists the log files stored at *%Temp%*\Microsoft Operations Manager:

TABLE A.1 Log Files at *%Temp%*\Microsoft Operations Manager

Log Name	Description
dllhost(B).mc8	The DAS is a server-based Component Object Module Plus (COM+) application hosted by the DLLHOST (server) process; the DLLHOST component controls access to the database. This log can help you determine why the DAS cannot connect to the database, which might appear as Administrator and Operator consoles being unable to connect. This log will also show when the DAS account is having permissions issues. To enable logging, see the "DLLHOST logging" section earlier in this appendix.
MOMAgentPerformanceHost-MOMLAB1(B).mc8	Provides information about what performance counters are being monitored and are returning data from the agent to the management server. The names of each counter and its value are displayed in the log.
MOMAgentScriptHost-MOMLAB1(B).mc8	Provides details about what scripts are running and some basic information about the script—such as whether any debug settings are set or whether debugging is even enabled for the script.
MOMService(B).mc8	Displays scan information including discovery rules, management group name, and the Action account name used with the scan. Scan successes and failures are logged so that when an agent is scanned and not found, a failure is logged. When the MOM service starts, it creates MOMService(Init).mc8. It will rename the (Init) file to MOMService(A).mc8. When MOMService (A).mc8 is full, it creates MOMService(B).mc8.
MOM.UI.OpsConsoleExe.log	MOM Operator console log file.
MOM.UI.OpsConsoleExe(####).log	If more than one instance of the Operator console is open, the log file will append the process ID (####) to the log file name.

TABLE A.1 Continued

Log Name	Description
MomConn2.log	Details connectivity information including whether a certificate is being used or user credentials are being used for the MOM Product Connector (MMPC). This logging is provided for the MOMConn Service. The MMPC is discussed in Chapter 19, "Interoperability."
MOMService.log	Captures the MOM Service discovery process (this is MOMService.log NOT MOMService.MC8).
MOMHost.log	Displays information about the capability of the MOMHost process to make connections to an agent, including its capability to connect to the remote registry and create/open keys. This log lists specific registry keys as well.
MOMHost_threads.txt	Provides a list of threads and process IDs so that individual entries in the logs can be associated with specific threads.
MCF.log	Displays information about the MOM Connector Framework when it is attempting to make a connection.

Table A.2 lists the log files stored at *%USERPROFILE%*\Local Settings\Temp\Microsoft Operations Manager.

TABLE A.2 Log Files at *%USERPROFILE%*\Local Settings\Temp\Microsoft Operations Manager

Log Name	Description
ManagementModuleUtil.mc8	Captures the import of .akm files using the ManagementModuleUtil.exe utility, discussed in Chapter 12, "Backup and Recovery."
mmc(B).mc8	Reflects activity in the MOM Administrator console.
mmc(Init).mc8	Reflects activity of starting the MOM Administrator console.
MsiExec.mc8	Displays information about the logging level and installation of MOM components when launched by running the MSI file itself. This file does not appear when Setup.exe is used to call the Windows Installer files for MOM.

Two installation log files are located on the management server at *%ProgramFiles%*\Microsoft Operations Manager 2005\AgentLogs and are described in Table A.3.

TABLE A.3 Log Files at *%ProgramFiles%*\Microsoft Operations Manager 2005\AgentLogs

Log Name	Description
MOMReporting.log	Updated with activity from MOM 2005 Reporting installation. When MOM Reporting setup completes successfully, this log is removed from the system.
MOMServer.log	Created by MOMServer.msi at install and includes activity from the installation of the management server.

MOM Trace Log Viewer

The MOM Trace Log Viewer (MOMLogViewer.exe) is part of the MOM 2005 Resource Kit and allows you to view the MOM trace log files ending with a .mc8 extension. The log viewer is a graphical utility that allows you to open and view multiple logs. It will refresh the contents of a window as it is being updated by the MOM Service component, allow you to filter the view, look at the detail for each line, search the log file, and mark specific lines for review. You can filter by thread, function name, trace level, or time span.

Event Processing

As discussed in several chapters in this book, MOM monitors activity by collecting and acting on events. As a managed computer generates events, MOM collects and processes the accumulated information. MOM 2005 uses three components as the foundation of its event processing architecture:

- Rules
- MOM agent
- Management server

We will discuss how each of these components is utilized.

Rules

Rules determine how MOM collects, processes, and responds to events as they occur. As described in Chapter 14, "Monitoring with MOM," rules enable you to filter operations data, including events, and send the filtered data to the management server. Rules are loaded into MOM with management packs, or you can create your own rules. After rules are established, MOM 2005 uses a specific process to pass the rules to agents to utilize in monitoring managed computers. This procedure involves the following steps:

1. The management server periodically queries the OnePoint database to check whether any rules have been updated or created. You can also force that check by committing configuration changes to apply rules immediately in the Administrator console by right-clicking on Management Packs in the Navigation pane and selecting Commit Configuration Change.

2. If new or updated rules are detected, the management server loads the rule(s) in its cache, where it remains until the next heartbeat. (Particulars of the heartbeat process are discussed in the "Heartbeat" section later in this appendix.)
3. When the management server receives a heartbeat event from an agent, it passes the changes to the agent.

The detailed data flow for these processes is described in the "Runtime Processing" section later in this appendix.

MOM Agent

The MOM agent stores rules in local cache on the managed computers. It also loads compiled rules from cache into random access memory (RAM) for rapid processing. As events occur, the agent compares each event to its list of rules. When there is a match, the agent performs the tasks specified by the rule. This could be one of the following actions:

- Ignore the event
- Report the event
- Create an alert
- Create a consolidated event
- Create a response

The agent sends its management server operational data for the events it has detected. Each agent uses a workflow manager, which channels the data into the proper processing queue. Events, alerts, and performance data are all handled by separate queues, which are stored in local queue files. The managers are discussed in the "Runtime Processing" section of this appendix.

Management Server

The management server receives the data from agents using the MOM Server component, which runs on the management server. The management server performs any tasks specified by the processing rules. Events are processed at the management server in three phases:

1. Collect data. The agent sends data such as encrypted events, consolidated events, and alerts using a default Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) port of 1270. The communication port can be modified if necessary in the Administrator console under Administration \ Global Settings \ Communications tab.
2. Process events. The management server loads rules from the OnePoint database into memory for more rapid execution. The rules are searched to find a match for the incoming stream of events and alerts. For each match, the management server

performs tasks described by the rule. This may include discarding the data, forwarding the data to the MOM database using the Data Access Service (DAS), and/or executing a response.

3. Store data. The management server saves all specified events and alerts in the OnePoint database through the DAS component.

Runtime Processing

The MOM runtime consists of the components hosted by the MOM services on both the management server and agent-managed computers. The management server includes the MOM Server and agent components; managed computers have only the agent component.

The MOM Server and agent share the same binaries and use the same set of subcomponents, which are also known as *managers*. A manager hosted by the MOM Server is described as running in a Server role; a manager hosted by the agent is known as running in an Agent role.

Figure A.1 shows the relationships between the components (managers) and how they connect between the MOM Server component and the agent. Notice that the only point of connection between the server and the agent is through the Communication Connector, meaning that all other components submit their data to the Communication Connector for processing.

These managers and their functions are as follows:

- Connector Manager—Controls the lifetime and interaction points with two roles for connectors—the data and configuration connector roles.

  In the data role, Connector Manager submits data it gets from the engine into the data connector and accepts configuration from the data connector.

  In the configuration role, Connector Manager submits configuration information into the configuration connector and accepts data from it.

  MOM agents only have a Communication Connector in the data connector role. MOM Servers use a Database Connector in the data connector role and a Communication Connector in the configuration connector role. The Connector Manager interacts with the Configuration Manager and the Queue Manager.

- Configuration Manager—Controls engine configuration information and updates engine components with new configuration information. The Configuration Manager is the common point for getting configuration-related services. This Manager interacts with Connector Manager, Action Manager, and the Executive.

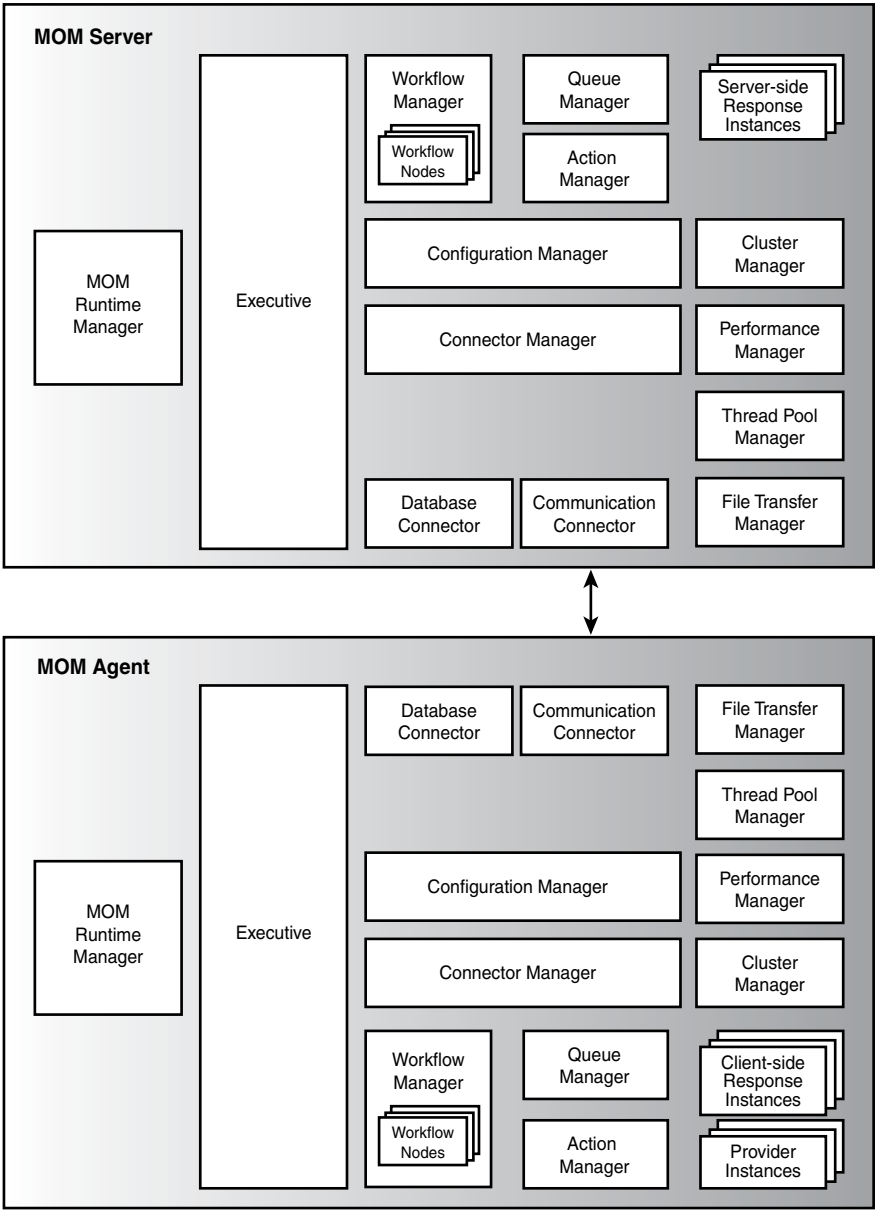


FIGURE A.1 MOM managers architecture.

- Action Manager—Action Manager controls the lifetime and interaction points with providers/responses, and supports interfaces that accept data from those providers/responses. It also provides Task execution services. Action Manager interacts with Queue Manager and Workflow Manager.

The Action Manager's lifetime is controlled by two interfaces, which initialize, start, stop, and shut down the Action Manager as required.

- Queue Manager—Controls engine queues. The Queue Manager has a fixed set of threads that process all data items inserted into the engine queue by giving the data item to the Workflow Manager. Queue Manager interacts with Workflow Manager.
- Workflow Manager—Controls the processing and lifetime of workflow nodes; supports sequential processing of operational data by passing through the workflow nodes. Workflow Manager using proxy nodes indirectly interacts with Connector Manager, Query Manager, and Action Manager.
- Thread Pool Manager—Implements scheduler functionality and a thread pool that is shared across all the managers.
- Cluster Manager—Discovers whether the managed node is a Cluster node and populates the list of virtual servers hosted by the node. The Cluster Manager actively monitors the virtual servers for failovers, servers coming online and going offline, and provides the basis for cluster management.
- File Transfer Manager—Communicates with Background Intelligent Transfer Services (BITS) to enable bidirectional file transfers requested by file transfer responses.
- Executive—Controls the lifetime of all the agents.

The MOM Engine

The MOM engine itself is a data structure that maintains the configuration required for a collection of managed computers. The same data structure is used on the MOM Server and the managed computer; the only difference between the two is that the data structure on the MOM Server tracks the number of agent-managed computers.

MOM Engine Data Structure

The following data is included in the MOM engine:

- A list of agent-managed computers, including the following information for each:

  Computer GUID (A GUID is a 128-bit value representing a Globally Unique Identifier.)

  Computer NetBIOS name

  Computer NetBIOS domain name

  Computer Fully Qualified Domain Name (FQDN)

  Agent configuration update time

  Agent settings

  Agent version

  Overrides

Flag indicating whether agent-managed or agentless managed

List of object GUIDs that refer to the rules, providers, scripts, and tasks an agent needs

List of task GUIDs and context for task targets. A task target controls the attributes available for passing to a command as parameters. It also controls which targets a task can be launched against.

- A list of rules targeted against the agents
- A list of provider instances used by the rules targeted against the agents
- A list of scripts referenced by the rules targeted against the agents
- A list of tasks that need to run on the agents

The management server uses the engine configuration data structure to build the engine configuration for a specific MOM agent, enabling the agent to know what to monitor and how to monitor its host computer. The local agent on the management server also uses this data structure to determine which computers are agentless managed.

Configuration Flow of the MOM Server

When a configuration change is implemented on the management server, a number of processes take place. Figure A.2 shows the communication flow from committing a configuration change, which is shown in the Windows Application event log as Event ID 21241.

Let's say you create a new rule and commit your configuration change using the MOM Administrator console. When a configuration change is initiated, two distinct processes occur—one on the server and the other on the client side by the agent. Figure A.2 shows the server-side process that takes place on the management server.

Let's look at the steps in this process:

1. The Database Connector calls the Connector Manager and submits a new configuration to the engine.
2. The configuration data is passed from the Connector Manager to the Configuration Manager.
3. The Configuration Manager will update a file with the cached configuration and makes a call (`IMCONTROL::Stop`) to stop the Action Manager. Action Manager needs to stop processing so that it can apply the configuration change to running components.

   The file updated by the Configuration Manager is the ConfigCache located at *%ALLUSERSPROFILE%*\Application Data\Microsoft\Microsoft Operations Manager\<*management group name*>\ConfigCache.
4. The Action Manager tells the Queue Manager (using the `IMOMControl::Stop` call) to stop processing items in the queue.

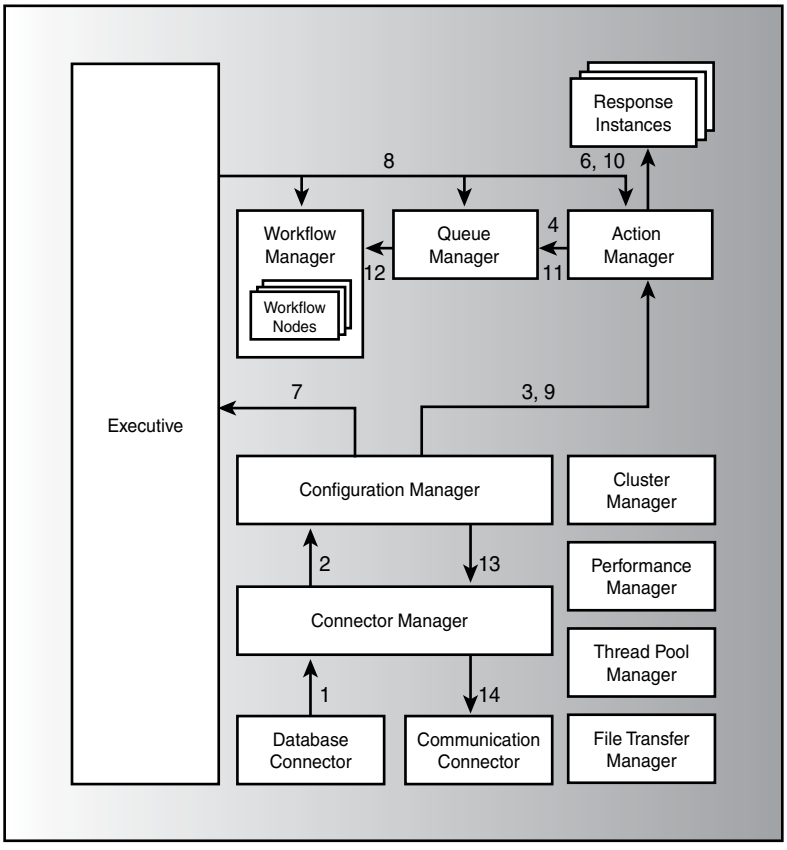


FIGURE A.2 Configuration change for the MOM Server.

5. The Queue Manager will suspend queue processing and make an `IMOMControl::Stop` call to the Workflow Manager, which stops the Workflow nodes. The Queue Manager continues to accept incoming data to insert into the queue.

6. The Action Manager makes a call to the stop (`IMOMControl::Stop`) and shut down (`IMOM::Shutdown`) methods on every started response.

   At this point, the Action Manager, Queue Manager, and Workflow Manager are fully stopped, although the Queue Manager continues to accept incoming data.

7. The Configuration Manager calls the Executive (`IMOMExecutive::NotifyConfigUpdate`) to broadcast a global configuration update notification.

8. The Executive notifies each manager of the configuration update.

9. The Configuration Manager tells the Action Manager to start, using the `IMOMControl::Start` call.

10. The Action Manager initializes responses on demand.
11. The Action Manager now tells the Queue Manager to Start, calling `IMOMControl::Start`.
12. The Queue Manager calls `IMOMControl::Start` on the Workflow Manager with an instruction to start the workflow nodes, and resumes queue processing.
13. The server-side configuration update is now complete.

    The Configuration Manager starts distributing new agent-side configurations—on agent heartbeat only—to agents that need to be updated, passing the prepared configuration for a given agent to the Connector Manager.
14. The Connector Manager passes the updated configuration to the Configuration Connector, which is the Communication Connector on the server side.

Configuration Flow of the MOM Agent

Now we'll look at the communication flow on the MOM agent when configuration changes are implemented, which is shown in Figure A.3. The managers on the agent perform functions similar to those performed on the Server component. Configuration information is passed from the management server to the agent during the heartbeat process.

The specific steps performed by the managers are as follows:

1. The Communication Connector calls the Connector Manager with `IMOMConnectorSink::IndicateConfig` and submits the new configuration engine to the engine.
2. The Connector Manager receives the configuration information and passes it to the Configuration Manager.
3. The Configuration Manager updates the ConfigCache file with the cached information and makes an `IMOMControl::Stop` call to stop the Action Manager for rule insertion.
4. The Action Manager calls stop methods and shutdown methods (`IMOMControl::Stop` and `IMOMControl::Shutdown`) on every running provider.
5. The Action Manager then instructs the Queue Manager to stop processing items from the queue, using the `IMOMControl::Stop` call.
6. The Queue Manager suspends queue processing and makes an `IMOMControl::Stop` call to the Workflow Manager, which stops the Workflow nodes. Insertion into the queues can continue, although processing is suspended.
7. The Action Manager calls stop methods and shutdown methods (`IMOMControl::Stop` and `IMOMControl::Shutdown`) on every started response.

   At this point the Action Manager, the Queue Manager, and the Workflow Manager are fully stopped.

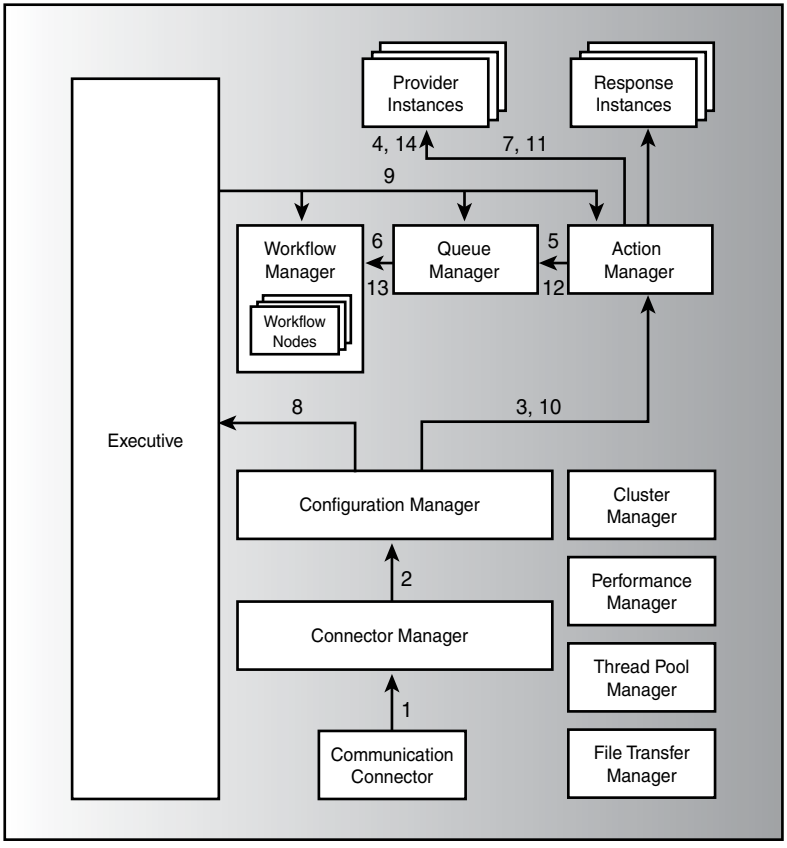


FIGURE A.3 Configuration change for the MOM Agent.

8. The Configuration Manager makes an `IMOMExecutive::NotifyConfigUpdate` call to the Executive to broadcast a global configuration update notification.
9. The Executive notifies each manager regarding the configuration update.
10. The Configuration Manager now tells the Action Manager to start, calling the `IMOMContol::Start` function.
11. The Action Manager initializes responses on demand—this is instead of calling initialization and start methods on responses.
12. The Action Manager tells the Queue Manager to start by initiating the `IMOMControl::Start` function.
13. The Queue Manager calls the Workflow manager with the `IMOMControl::Start` instruction to start the workflow nodes and resume queue processing.
14. The Action Manager calls the initiation and start methods (`IMOMControl::Init` and `IMOMControl::Start`) on the new providers, and the configuration update is finished—every component is now started and operational.

Data Types

The MOM runtime component monitors applications based on the specified configuration and sends operational data to the Database Connector. Many of these data types have been discussed elsewhere in this book; here we will list each data type used by the runtime:

- Event dataitem—Represents an event in the engine.
- Performance dataitem—Represents performance data in the engine.
- Alert dataitem—An alert or an update to an existing alert in the engine. An alert dataitem also represents a response dataitem.
- Response dataitem—Contains information indicating that the response to a given rule should be triggered.
- Discovery dataitem—Contains service discovery information.
- Workitem—Dataitems flow inside a workitem in the engine. The workitem contains additional information about the dataitem, such as the computer the dataitem is generated for. The workitem also contains annotations added by the engine, which specify how the dataitem should be handled within the Workflow nodes and connectors.

MOM Agent Data Flow

After an agent receives configuration data from the management server it begins to collect and submit data based on the rules and responses provided. Figure A.4 shows the specific processes and steps for the data flow among components in the MOM agent.

The data flow process for the agent is as follows:

1. When a specified event occurs, a provider or response instance calls the appropriate method—to process or submit data—to send data to the Action Manager.
2. The Action Manager creates internal workitems for engine processing. If the original call was to process data, the Action Manager calls a process method on the Workflow Manager. If the original call was to submit data, the Action Manager calls a submit method on the Queue Manager.
3. The Queue Manager puts the workitem in the queue, and later dispatches a thread that picks up the workitem from the queue and calls a process method on the Workflow Manager.
4. The Workflow Manager processes data through the agent workflow nodes. When there is a rule match, the Communication node—acting as a proxy for the Connector Manager—passes data to the Connector Manager.
5. The Connector Manager passes data to the data connector. The data connector is the agent-side communication connector.

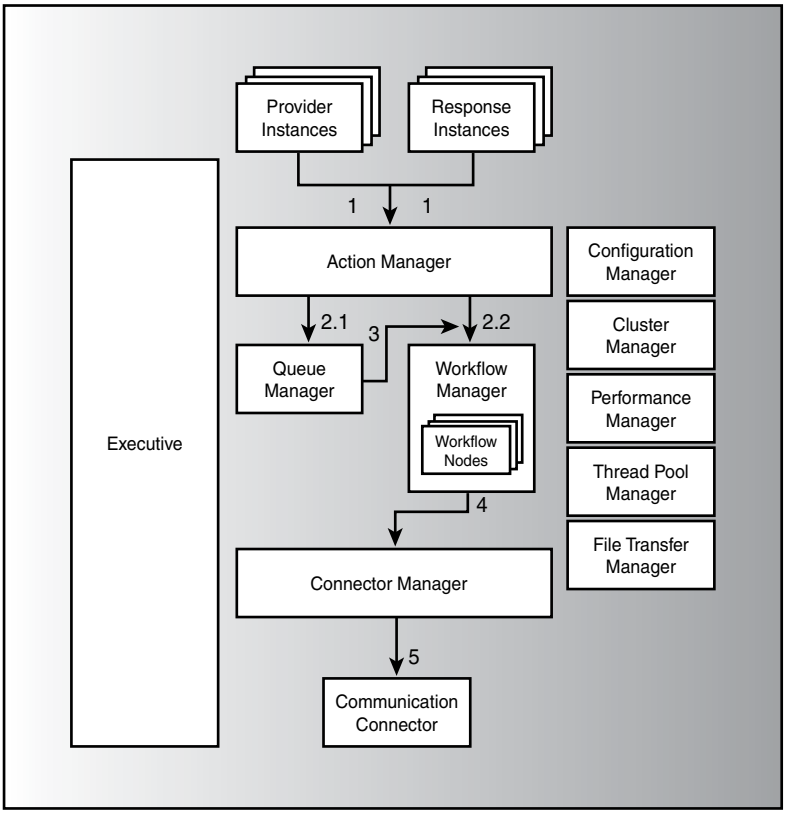


FIGURE A.4 MOM Agent data flow.

MOM Server Data Flow

Now let's look at the data flow among components in the MOM Server in Figure A.5. This should appear somewhat like reverse-order to the MOM agent data flow, with the addition of the Database Connector.

1. The server-side Communication Connector, acting in the role of a configuration connector, receives data from the agent connector (which is the Communication Connector on the client) and calls a method on the Connector Manager to submit data to the engine.
2. The Connector Manager redirects the previous call to a submit method call on the Queue Manager.
3. The Queue Manger uses the submit method to put workitems in the queue and will dispatch a thread to pick up the workitem from the queue and call a process on the Workflow Manager.
4. The Workflow Manager processes data through the server workflow nodes, where the last node is a proxy database node that redirects calls to the Connector Manager.

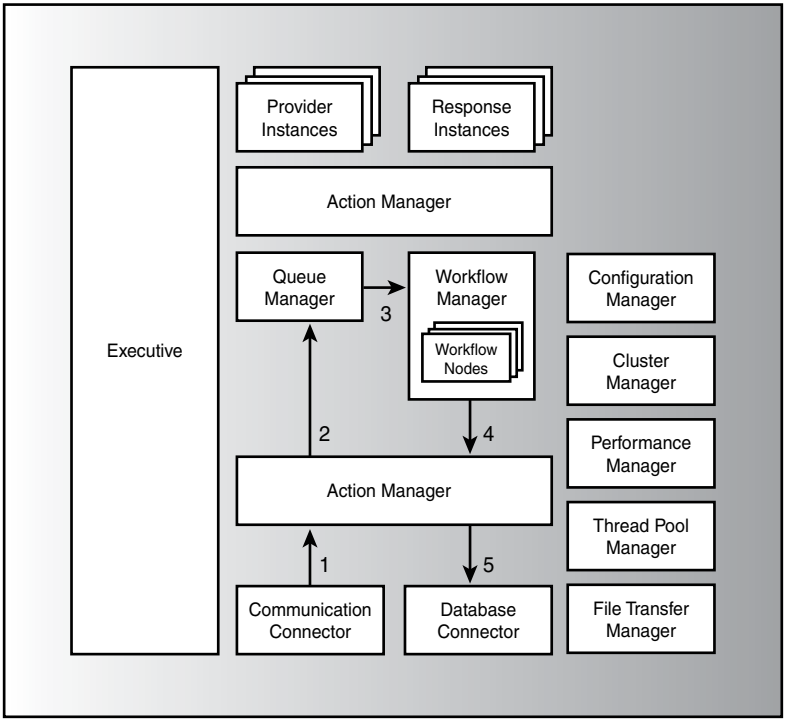


FIGURE A.5 MOM Server data flow.

5. The Connector Manager passes the data to the data connector, which is a server-side database connector.

Earlier we referred to the heartbeat. The heartbeat is the means used to notify the management server that its agents are alive and is a key piece of agent functionality.

Heartbeat

During Heartbeat, the Agent Communication Connector sends heartbeat messages to the management server to let it know that the agent is available. When an agent is on the Active node of a cluster, it also sends a second heartbeat every 10 seconds for the virtual cluster name. Heartbeat messages consist of small UDP packets containing the GUID of the agent and a time stamp. By default, a heartbeat is sent every 10 seconds. This is configurable in the Administrator console under Administration \ Global Settings \ Agents \ Agent Heartbeat tab, displayed in Figure A.6.

The Agent Heartbeat tab also shows that the current heartbeat scan interval for management servers is 30 seconds. You can modify this interval under the Administration \ Global Settings \ Management Servers \ Heartbeat Checking tab. The settings here include Heartbeat Scan and Heartbeat Ping. The heartbeat scan must be longer than the heartbeat interval on the agent (as defined in Figure A.6). Using the default settings for

heartbeat scan, the primary management server for an agent will check every 30 seconds to see whether it has received a heartbeat from each agent it is responsible for. If an agent does not respond with at least one heartbeat during that 30-second window, the management server decreases an internal counter used to track agents that are not heartbeating.

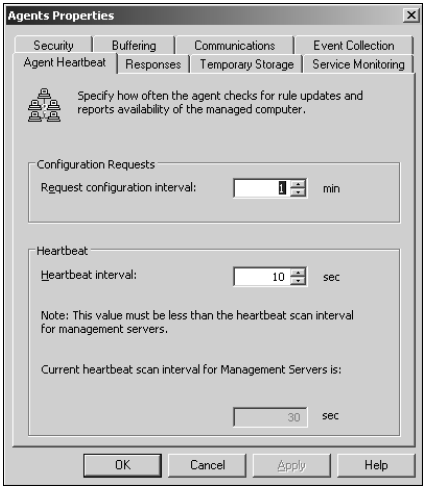


FIGURE A.6 Agent heartbeat settings.

After three consecutive missed heartbeats—defined in the Heartbeat Ping section of the screen as the number of scans before generating service unavailability and in this case a maximum of 90 seconds—the counter will be at zero. At this point the management server then tries to ping the client. If the ping is successful, Event ID 21284 is generated indicating that the agent failed to heartbeat but responded to the ping. If the ping is unsuccessful, MOM generates Event ID 21285, which indicates that the machine is offline. Figure A.7 shows the Heartbeat Checking settings.

Sending Packets

Heartbeat packets are sent using UDP, which means they are transactionless; the agent sends the packet and does not check to see whether the data is delivered or acknowledged. UDP packets have less overhead than TCP, which requires an acknowledgement.

Ignoring Missing Heartbeats ... and Then Some

In the original (Release to Manufacturing [RTM]) version of MOM 2005, turning on the Ignore Missing Heartbeats option for a computer under Administration \ Computers \ Agent-Managed Computers or Administration \ Computers \ Agentless Managed Computers not only ignores missing heartbeat, but the management server does not process any alerts received from the agent, and the alerts are not added to the OnePoint database.

The Ignore Missing Heartbeats option erroneously put the MOM agent into maintenance mode, which means by definition that any alerts generated by the agent are not processed or added to the database.

This situation is corrected with MOM 2005 Service Pack 1. For further information see http://support.microsoft.com/kb/889071/.

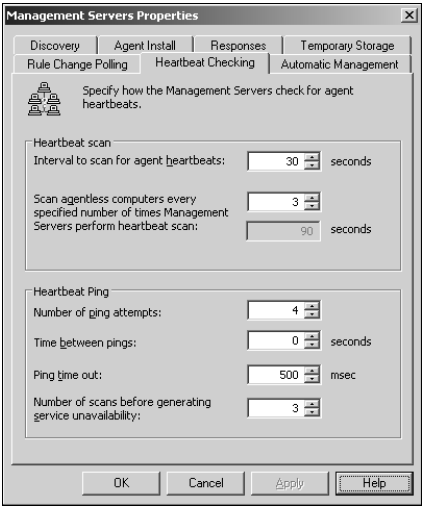


FIGURE A.7 Management server heartbeat configuration.

Failover Processing by Agent

If there are multiple management servers and for some reason the agent cannot contact its designated (primary) management server, it attempts to fail over to another management server. As long as the agent can submit heartbeats, it will submit them to this server until it determines that its designated management server is again available.

The agent performs a configuration update every 60 seconds. The configuration update is transaction based, enabling the agent to determine whether the configuration data has originated from its designated management server. When the designated server becomes available, the agent switches back to that server with its next heartbeat.

TCP is used for reliable communications when the agent has an alert or other information to send to the management server. If the agent sends this data to a management server other than its designated one, the operational state of the agent will indicate an error condition.

Events 21249 and 21250 on the Agent

If you are experiencing intermittent network problems, you may notice events 21248 and 21250 being regularly logged in the Application event log on the agent. Event 21259 indicates the agent failed over to another management server, and 21250 indicates the agent reestablished a connection to its primary server.

What has happened is the agent is failing over to the secondary without retrying its connection to the primary. This can lead to failover or fallback loops when you have transient network issues.

This behavior is resolved with MOM 2005 Service Pack 1. If you are not able to apply the service pack, a registry fix is available, which is documented at http://support.microsoft.com/kb/892920/. The setting will indicate how many times the agent retries the management server before failing over, with a default setting of three tries.

Management Server Tracking

The Server Communication Connector on the management server tracks availability of MOM agents by processing heartbeat messages submitted by the agent's Communication Connector. The server-side Communication Connector keeps a table listing all computers managed by the server, including the last time of contact, and will notify the Database Connector for the database to be updated with the last contact time.

A separate thread checks the table to determine whether an agent has missed a set number of heartbeats, as discussed earlier in the "Heartbeat" section of this appendix. Should this happen, a ping job is added to a queue, which is processed by Pinger Threads.

Pinger Threads

Pinger Threads work through a list of computers that do not appear to be submitting Heartbeat data to determine whether the problem is availability or alternatively the MOM Service component is not performing its Heartbeat function. Depending on the results of the Ping job, the connector generates one of the following events:

- Agent stopped heartbeating (Event ID 21209).
- Agent stopped heartbeating because the computer is not available (Event ID 21285).
- Agent stopped heartbeating because the service is not available (Event ID 21284).

Rules on the management server use these events to generate status alerts regarding the agent's availability. Additionally, you can confirm the status of an agent by checking the State view in the Operator console, where green indicates that an agent is available and red indicates an unresponsive agent. You can also search for Event IDs 21209, 21284, and 21285, which indicate heartbeat failure. A reestablished heartbeat generates Event ID 22086. Event ID 21210 indicates the machine is available.

Agent Helper Utility

The MOM Agent Helper is part of the MOM 2005 Resource Kit and allows you to manage agents when no heartbeat is present by restarting the agents and reinstalling them if necessary. The resource kit utility includes a DLL and a sample management pack (.akm file) that shows how to configure the two main responses of ReviveAgent and ReviveDeadAgent.

The Agent Helper requires that Server Side Includes be enabled. Documentation on the Agent Helper can be found with the Resource Kit, which is available at http://go.microsoft.com/fwlink/?linkid=34629. Remember that the MOM 2005 Resource Kit is not supported by Microsoft.

MOM Agent Monitor Utility

Although getting a heartbeat from an agent typically means that the agent is working, occasionally a heartbeating agent does not send events or performance data to the management server. You can use the MOM Agent Monitor Management Pack available from the gotdotnet code gallery to test the end-to-end functionality on the MOM agents. The management pack writes events at each agent and waits for them to be received by the MOM Server.

The MOM Agent Monitor can be downloaded from the code gallery at www.gotdotnet.com. Click on the Code Gallery, select directory, and at the Projects Directory search for "MOM Scripts." Select the MOM Scripts project and download the zip file containing the MOM Agent Monitor.

On the CD

The MOM Agent Monitor is included on the CD with this book.

Summary

This appendix took an in-depth look at some of the inner workings of MOM 2005. We examined key registry settings and defined a number of files used by MOM. We also looked at how MOM processes events. We discussed MOM's runtime architecture, including the MOM engine and heartbeat processing. This discussion should have given you a better understanding of how MOM functions.

APPENDIX B

Registry Settings

IN THIS APPENDIX

The Windows Registry is a hierarchical "database" that stores information about how the operating system and applications on a computer run. The Registry is organized in a tree format and can be viewed using the Registry Editor program, regedit.exe.

About the Registry

Folders seen in regedit represent keys and are displayed in the left side or Navigation area in the Registry Editor window. There are five folders, or predefined keys:

- HKEY_CURRENT USER (HKCU)—Contains root of configuration information for the currently logged-on user. This information is referred to as a user's *profile*.
- HKEY_USERS (HKU)—Contains the root of all user profiles on the computer. The HKEY_CURRENT_USER folder is actually a subkey of HKEY_USERS.
- HKEY_LOCAL_MACHINE (HKLM)—Contains configuration information particular to the computer which can be used by any user.
- HKEY_CLASSES_ROOT (HKCR)—A subset of information in HKEY_LOCAL_MACHINE. Information stored here ensures the correct program will open when you open a file using Windows Explorer. It contains the linking between executable programs and the program extensions used by data files on the system.
- HKEY_CURRENT_CONFIG (HKCC) —Contains configuration data for the current hardware profile. The SYSTEM subkey contains a subset of the information (the CurrentControlSet) that is a subkey of HKEY_LOCAL_MACHINE\SYSTEM.

Every database has physical files stored on disk that hold the data you view. The physical files used by the Registry are called *hives* and are loaded by Windows at system startup. The hive files are stored in the *%systemroot%*\system32\config folder of your system. Table B.1 shows the relationship between the hive files and their corresponding Registry keys.

TABLE B.1 Hive Files and Corresponding Registry Keys

Hive File Name	Registry Key
Default	HKEY_USERS\DEFAULT
SAM	HKEY_LOCAL_MACHINE\SAM
Security	HKEY_LOCAL_MACHINE\SECURITY
Software	HKEY_LOCAL_MACHINE\SOFTWARE
System	HKEY_LOCAL_MACHINE\SYSTEM

As shown in Table B.1, most of the hives are subkeys of HKEY_LOCAL_MACHINE. The exception is the Default hive, which is the default user profile.

The hive for the current logged-on user profile, HKEY_CURRENT_USER, is the ntuser.dat file stored within *%systemdrive%*\documents and settings\<*user name*>. There is also a Hardware subkey for HKEY_LOCAL_MACHINE. This hardware "hive" is dynamically built at system startup and is not stored on disk.

Other files stored at *%systemroot%*\system32\config include:

- Pristine versions of the five Registry hive files, which have an extension of .SAV. These are never-modified hive files for the corresponding keys, created when Windows was installed on the system.
- Windows-created backup files for the hive files, with a .LOG extension.
- The Windows event log files, with an extension of .EVT. The number of .EVT files on any particular system will vary based on the computer's role. For example, domain controllers, DNS (Domain Name System), and FRS (File Replication Service) servers have additional event logs.

Additional information about the registry is available at http://support.microsoft.com/kb/256986/, "Description of the Windows Registry," and http://support.microsoft.com/kb/322756/, "How to back up, edit, and restore the registry in Windows XP and Windows Server 2003." Incorrectly modifying the Registry may render your system unusable, so you should always make a backup of the Registry or its subkeys prior to making changes.

Microsoft Operations Manager-Related Registry Keys

The keys used by Microsoft Operations Manager (MOM) 2005 are found in the software hive of the registry under the Mission Critical Software subkey. The product that became MOM was originally developed as a monitoring system by Mission Critical Software. After that company was acquired by NetIQ, the Operations Manager technology was licensed to Microsoft in October 2000.

The first two versions of MOM have maintained the Mission Critical Software subkey and the original name of the operating database, OnePoint. Microsoft intends to phase out these references in the next version of Operations Manager.

Under the HKEY_LOCAL_MACHINE\SOFTWARE\Mission Critical Software subkey are two child subkeys: DASServer and OnePoint. Table B.2 briefly documents some of the more interesting entries located under the Mission Critical Software subkey.

TABLE B.2 MOM 2005 Registry Keys

Key Name	Name	Type	Data	Description
HKLM\SOFTWARE\Mission Critical Software	TraceLevel	REG_DWORD	0x1	The higher the level, the more detail appears in the .mc8 log. Note level 0 still does some logging. Specify -1 (that is, FFFFFFFF) to turn logging off. Possible values range from 9 to -1. The value is set to 1 for new MOM installations. If you upgraded from an earlier version, the previous TraceLevel value is retained. TraceLevel logging is documented at http://support.microsoft.com/kb/923104/.
	TraceCircularLines	REG_DWORD	0xc350	How big, in lines, the log will get before it wraps. Default 50,000 lines.
	TraceInitSeconds	REG_DWORD	0x3c	How many seconds to log to "init" file before starting circular log. Default 60 seconds.
HKLM\SOFTWARE\Mission Critical Software\DASServer	AuditingFlags	REG_DWORD	0	Boolean to turn DAS auditing on/off. 0=off, 1=on.
	LoggingFlags	REG_DWORD	0xffff	Bit flags to turn on/off different levels of DAS logging. Any combination of bits can be specified. To turn on full DAS logging, the value should be 0x3F. Off by default.
	Database	REG_SZ	OnePoint	Name of database on the SQL Server. For MOM 2005 equals "OnePoint."
	DataSource	REG_SZ	Example: MONARCH	Name of the SQL Server the local DAS points to.
HKLM\SOFTWARE\Mission Critical Software\OnePoint	IsConsolidator	REG_SZ		This value is used to prevent an agent from being installed on a management server. Presence or absence of "IsConsolidator" value denotes whether a local machine is a management server.
	EnableErrorReporting	REG_DWORD	0	Enables sending error reporting to Microsoft.

TABLE B.2 Continued

Key Name	Name	Type	Data	Description
	ManualAgent	REG_SZ	Configure	Controls how much the MOM Server will do to this computer. When you do a manual agent install, you can set it so that the MOM Server takes full control or does nothing. All management servers are set to Configure. Possible values are: Full, Configure, and Group.
	CrashOnAllocationFailure	REG_DWORD	0	Turned off.
	ServiceVersion	REG_SZ	5.0.2911.0	Version of Microsoft Operations Manager. MOM 2005 SP1 is 5.0.2911.0, and MOM 2005 is 5.0.2749.0. Earlier versions are documented at http://support.microsoft.com/kb/923105/.
	TempDir	REG_SZ	*%TEMP%*	Location of Temp directory.
	DataDir	REG_SZ	*%ALLSUSERSPROFILE%* \ Application Data\ Microsoft\Microsoft Operations Manager\	Location of Data directory.
	MaxServerPrivateBytes	REG_DWORD	0x12c00000	The MOM Service process (MOMService.exe) will restart if private bytes exceed this setting, by default 300MB.
	BootStartupDelay	REG_DWORD	0x3c	60 seconds.
	MaxDefaultHostPrivateBytes	REG_DWORD	0x6400000	Maximum memory for a MOM 2005 agent to use; default is 100MB.
	MaxScriptHostPrivateBytes	REG_DWORD	0x6400000	Host process for script responses; default is 100MB. If you are receiving event 21246, you may also want to read KB article 891605, http://support.microsoft.com/kb/891605/.

TABLE B.2 Continued

Key Name	Name	Type	Data	Description
	EnableActiveDebugging	REG_DWORD	0x1	Enable script execution logging. Log files are written to *%windir%*\temp\Microsoft Operations Manager\AgentResponses-<*management group name*>.log.
	DebugEnabledScripts	REG_SZ	*	Specifies scripts permitted to be debugged. The default "*" is a wild card specifying all scripts. You can modify this value to the name of a specific script to be debugged, a list of script names separated with commas, or a more specific string containing a wild card. Specifying a value does not prevent other scripts from executing on the MOM agent, but the debugger will catch the script only if it matches one of the values in the registry key.
HKLM\SOFTWARE\Mission Critical Software\OnePoint\Configurations			Example: Group1	There is a subkey for every MOM configuration (management) group, which corresponds to a MOM database.
HKLM\SOFTWARE\Mission Critical Software\OnePoint\Configurations\<*management group name*>	ConfigGuid	REG_SZ	varies	Version number of the latest installed management server. The Globally Unique Identifier (GUID) is generated at runtime by the setup program and is associated with the group name.
HKLM\SOFTWARE\Mission Critical Software\OnePoint\Configurations\<*management group name*>\Operations	Database	REG_SZ	Example: MONARCH	Default SQL Server the Administrator console MMC points to.

TABLE B.2 Continued

Key Name	Name	Type	Data	Description
HKLM\SOFTWARE\Mission Critical Software\ OnePoint\Configurations\ <*management group name*> \Operations\Agent	MaxFileSize	REG_DWORD	0x3a98	Decimal is 15000. Total number of bytes used by all queues combined on the agent.
	NumResponseThreads	REG_DWORD	0xa	Number of threads to process alerts and response items in the response queue.
	ContactThreshold	REG_DWORD	0xe10	Default 10.
	FileLocation	REG_SZ	*%default%*	Defines the location of the agent queue file; by default points to %*SystemDrive*%\Documents and Settings\All Users\Application Data\Mission Critical Software\ OnePoint\<*management group name*>.
	AgentlessProvidersOFF	REG_DWORD	0	Agentless managed toggle.
	AllowProxyForwarding	REG_DWORD	0	Proxy forwarding toggle.
	CollectBinaryData	REG_DWORD	0	Collect Binary Data.
	ConfigRequestInterval	REG_DWORD	0x3c	60 seconds.
	GlobalVdirLocation	REG_SZ		Empty.
	MaintenanceMode	REG_DWORD	0	Toggle Maintenance Mode off or on.
	MaxAlertCount	REG_DWORD	0x32	Contains the number of alerts a rule can generate in the specified time (default 50). Used to prevent alert storms.
HKLM\SOFTWARE\Mission Critical Software\ OnePoint\Configurations\ <*management group name*>\Operations\ Consolidator	SocketSecurePort	REG_DWORD	1270	Represents the secure port used for communications between the agent and the management server.
	Heartbeat	REG_DWORD	10	Specifies the interval that the agent uses to submit information to the management server.

This page intentionally left blank

APPENDIX C

Performance Counters

MOM collects a number of performance counters for the agent (monitored computer), management server, and MOM-to-MOM Connector Service. These counters are installed when the corresponding component (agent, management server, Connector Service) is installed on a computer.

IN THIS APPENDIX

Counters Maintained by the Monitored Computer

TABLE C.1 Agent Counters (These are all per management group)

Counter	Description
Comm Alert Proc Avg Time	Specifies average time (in milliseconds) an alert spends in the Communication Connector on an agent.
Comm Alert Proc Inc Rate	Specifies number of alerts that have arrived at the Communication Connector on an agent between Time T1 and time T2.
Comm Alert Proc Simple Count	Specifies total number of alerts in the Communication Connector on an agent at a particular time.
Comm Alert space percent used	Specifies percent of Alert Communication Connector queue in use. This setting is configurable by the user. The Alert Communication Connector queue comprises one-third of the overall agent queue file.
Comm Data Proc Avg Time	Specifies average time (in milliseconds) data spends in Communication Connector on an agent. Data refers to performance, events, or discovery events.
Comm Data Proc Inc Rate	Specifies incoming rate of data in the Communication Connector on an agent between Time T1 and Time T2.
Comm Data Proc Simple Count	Specifies total number of alerts in the Communication Connector on an agent at a particular time.
Comm Data Proc percent used	Specifies percent of Data Communication Connector queue use. This setting is configurable by the user. The Data Communication Connector queue comprises one-third of the overall agent queue.
Queue Process Avg Time	Specifies average time (in milliseconds) items (data and alerts) spent in the Workflow queue on an agent.
Queue Process Inc Rate	Specifies incoming rate of items (data and alerts) into the Workflow queue on an agent between Time T1 and Time T2.
Queue Process Simple Count	Specifies total number of items (data and alerts) in the Workflow queue on an agent at a particular time.
Queue space percent used	Specifies percent of the Workflow queue in use (by data and alerts). This setting is configurable by the user. The Workflow queue comprises one-third of the overall agent queue size.
Resp Exec Avg Time	Specifies average time (in milliseconds) a response spends on an agent. Responses are launched through rules and include scripts and command-line responses.
Resp Exec Inc Rate	Specifies incoming rate of responses on an agent between Time T1 and Time T2. Responses are launched through rules and include scripts and command-line responses.

TABLE C.1 Continued

Counter	Description
Resp Exec Simple Count	Specifies total number of responses being processed on an agent at a particular time. Responses are launched through rules and include scripts and command-line responses.
Task Exec Avg Time	Specifies average time (in milliseconds) a task requires on an agent. Tasks are launched by users in the Operator console.
Task Exec Inc Rate	Specifies incoming rate of tasks on an agent between Time T1 and Time T2. Tasks are launched by users in the Operator console.
Task Exec Simple Count	Specifies total number of tasks being processed on an agent at a particular time. Tasks are launched by users using the Operator console.
Workflow avg time	Specifies average amount of time (in milliseconds) items (data and alerts) spend in the Workflow queue on an agent.
Workflow inc rate	Specifies incoming rate of items (data and alerts) into the Workflow queue on an agent between Time T1 and Time T2.
Workflow simple counter	Specifies total number of items (data and alerts) in the Workflow queue on an agent at a particular time.

Counters Maintained by the Management Server

TABLE C.2 Management Server Counters (These are all per management group)

Counter	Description
DB Alert Insert Avg Time	Specifies average time (in milliseconds) that alerts take to be inserted into the MOM database.
DB Alert Insert Inc Rate	Specifies incoming rate of alerts that are to be inserted into the MOM database between Time T1 and Time T2.
DB Alert Insert simple count	Specifies total number of alerts that are being inserted into the MOM database at a particular time.
DB disc insert avg time	Specifies average time (in milliseconds) that discovery data takes to be inserted into the MOM database.
DB disc insert inc rate	Specifies incoming rate of discovery data items that are to be inserted into the MOM database between Time T1 and Time T2.
DB disc insert simple count	Specifies total number of discovery data items that are being inserted into the MOM database at a particular time.
DB event Insert Avg Time	Specifies average time (in milliseconds) that events take to be inserted into the MOM database.
DB event Insert Inc Rate	Specifies incoming rate of events that are to be inserted

TABLE C.2 Continued

Counter	Description
	into the MOM database between Time T1 and Time T2.
DB event Insert simple count	Specifies total number of events that are being inserted into the MOM database at a particular time.
DB perf insert avg time	Specifies average time (in milliseconds) that performance items take to be inserted into the MOM database.
DB perf insert inc rate	Specifies incoming rate of performance items that are to be inserted into the MOM database between Time T1 and Time T2.
DB perf insert simple count	Specifies total number of performance items that are being inserted into the MOM database at a particular time.
Queue Process Avg Time	Specifies average time (in milliseconds) items (data and alerts) spend in the Workflow queue on a management server.
Queue Process Inc Rate	Specifies incoming rate of items (data and alerts) into the Workflow queue on a management server between Time T1 and Time T2.
Queue Process Simple Count	Specifies total number of items (data and alerts) in the Workflow queue on a management server at a particular instance in time.
Queue Space Percent used	Specifies percent of the Workflow queue in use (by data and alerts). This setting is configurable by the user and comprises 100% of the overall server queue.
Resp Exec Avg Time	Specifies average time (in milliseconds) a response requires on a management server. Responses are launched through rules and include scripts and command-line responses.
Resp Exec Inc Rate	Specifies incoming rate of responses on a management server between Time T1 and Time T2. Responses are launched through rules and include scripts and command-line responses.
Resp Exec Simple Count	Specifies total number of responses being processed on a management server at a particular time. Responses are launched through rules and include scripts and command-line responses.
Task Exec Avg Time	Specifies average time (in milliseconds) a task requires on a management server. Tasks are launched by users using the Operator console.
Task Exec Inc Rate	Specifies incoming rate of tasks on a management server between Time T1 and Time T2. Tasks are launched by users in the Operator console.
Task Exec Simple Count	Specifies total number of tasks being processed on a management server at a particular time. Tasks are launched by users in the Operator console.
Workflow avg time	Specifies average time (in milliseconds) items (data and

TABLE C.2 Continued

Counter	Description
	alerts) spend in the Workflow queue on a management server.
Workflow inc rate	Specifies incoming rate of items (data and alerts) into the Workflow queue on a management server between Time T1 and Time T2.
Workflow simple counter	Specifies total number of items (data and alerts) in the Workflow queue on a management server at a particular time.

Counters Maintained by the MOM-to-MOM Connector Service

TABLE C.3 MOM-to-MOM Connector Service Counters

Counter	Description
New Alert forwarding Rate	This is the number of alerts forwarded per second.
Total new alerts forwarded	This is the total number of alerts forwarded. It increases steadily until the MOM Connector Service restarts.

This page intentionally left blank

APPENDIX D

Database Views

IN THIS APPENDIX

Microsoft does not support direct access to the tables in the MOM databases due to potential conflicts and performance issues. Microsoft also reserves the right to change the underlying table structure at any time and does not publish the database schema. In this appendix, we cover the views available to access the operations and reporting databases.

SDK SQL Views—Accessing Operational Data

The MOM Software Development Kit (SDK) contains views you can use to access the OnePoint operations database. This is the only supported method of accessing the MOM 2005 operations database via SQL queries.

The MOM operations database supports the views listed in Table D.1.

TABLE D.1 Operations Database Views

SDK SQL View	Description
SDKAlertsAndEventsView	Correlates each alert to the event that caused it. The relationship between events and alerts is not always a simple one-to-one, cause-and-effect relationship. Although an alert must have at least one event, several events might be associated with a single alert. This is the case when several similar events, called an *event storm*, are consolidated by MOM. More than one alert can be raised by a single event. The alert and event Globally Unique Identifiers (GUIDs) can be used to identify and correlate specific alerts and events from other views, such as SDKAlertView, SDKEventView, and SDKAlertsAndEventsView.
SDKAlertView	Displays the history and properties of the alerts created by MOM. Both resolved and unresolved alerts are included in this view.
SDKComputerAttributesView	Represents all computer attributes collected from the Windows registry and other supported attribute sources.
SDKComputerGroupView	Represents the computer groups used to manage agent computers.
SDKComputerToComputerGroupView	Associates computers and computer groups. For information about the computers and the computer groups, see the SDKComputerView and SDKComputerGroupView, respectively.
SDKComputerView	Stores data about all the computers in the MOM database. This includes all computers with MOM agents and any computers running MOM components or the computer running SQL Server that is hosting the MOM database. Note that the SDKComputerView in the operations database will not return computers that appear to be invalid or deleted. The SDKComputerView included in the reporting database could return some computers that were not returned by the corresponding view in the operations database.
SDKEventParametersView	An SQL view that displays information about the parameters of a MOM event.
SDKEventView	Displays the properties of events captured by MOM. Note that the SDKEventView included in the MOM operations database does not return events that appear to be invalid, such as events associated with unrecognized or deleted computers. The SDKEventView included in the reporting database does not filter events in the same way, and it could return some events that were not returned by the corresponding view in the operations database.

TABLE D.1 Continued

SDK SQL View	Description
SDKPerformanceView	An SQL view that stores performance counter data from the computers managed by MOM.

Figure D.1 shows the SQL views and the associations between them. As you can see from this diagram, the SDKComputerView is the central view that the other views are related to and through.

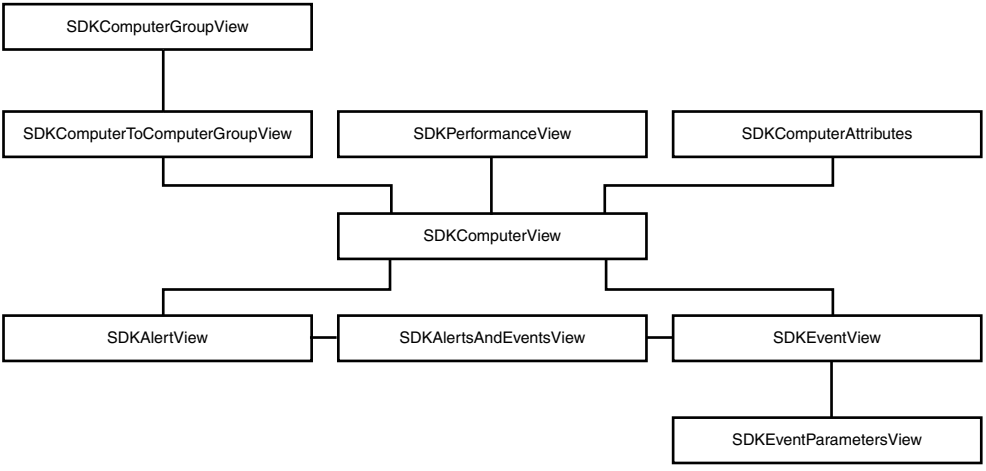


FIGURE D.1 SDK SQL view relationships.

Data in views is dynamic. The data is populated from the database tables at the time that a query runs, so the data in a returned query is always current. The view columns are also generated from a number of tables that were separated for performance purposes, giving a more coherent view of the relevant information while requiring less knowledge of the underlying data structures. Although Microsoft reserves the right to change the base table structure at any time, views are more stable and usually persist between versions, providing better supportability to applications using them.

The SDK SQL views are read-only and do not provide the capability of writing to the MOM 2005 database. If you need to write to the database, you will need to do so programmatically using the Management Server Class Library (MCL) or the Windows Management Instrumentation (WMI) classes.

To grant access to the SDK SQL views, you can add the user's Windows account as a database user for the OnePoint operations database and assign the database user the MOM SDK View User database role.

The MOM 2005 SDK documentation includes extensive references to the MOM SDK Views and is available at http://go.microsoft.com/fwlink/?linkid=50272.

SQL Views—Accessing Archival Data

Access to the long-term historical data in the reporting database is also available using SQL views. These SQL views are much more extensive than the SDK views that provide access to the operations database. The database schema of the reporting database is different from the operations database, being fundamentally optimized to store large quantities of archival information and provide efficient querying of the data.

The SQL views for the reporting database are listed in Table D.2. As you can see, there are 28 different views, as compared to the nine SDK views for the operations database. These views provide a wealth of data for generating reports. The views are prefaced by the "SC" acronym, which stands for "System Center," and are used by MOM 2005 Reporting to generate reports.

TABLE D.2 Reporting Database Views—Rules

SQL View	Description
SC_AlertFact_View	Represents all alerts currently in the MOM reporting database.
SC_AlertHistoryFact_View	Stores a copy of an alert at a point in time when the alert was modified, either by a user or by MOM.
SC_AlertLevelDimension_View	Stores alert severity levels.
SC_AlertResolutionStateDimension_View	Represents an alert resolution state. Custom resolution states can be defined in MOM.
SC_ClassAttributeDefinitionDimension_View	Represents the class attribute definitions.
SC_ClassAttributeInstanceFact_View	Represents the class attribute instances.
SC_ClassDefinitionDimension_View	Represents information about the extensible classes, or types, that can be defined in MOM 2005.
SC_ClassInstanceFact_View	Represents the class instances.
SC_ComputerDimension_View	Stores information about computers, including MOM servers, clients with MOM agents, clients without MOM agents, and any other computer that serves as a source for events or alerts.
SC_ComputerRuleDimension_View	Represents a computer discovery rule.
SC_ComputerRuleToProcessRuleGroupFact_View	Associates rule groups to computer rules.
SC_ComputerToComputerRuleFact_View	Associates rules with managed computers.

TABLE D.2 Continued

SQL View	Description
SC_CounterDetailDimension_View	Represents the performance counter used by a performance rule.
SC_EventDetailDimension_View	Represents event properties beyond those found in the SC_EventFact_ View.
SC_EventFact_View	Represents the events that MOM either collects or generates.
SC_EventTypeDimension_View	Is used to describe the type, or severity, of an event.
SC_ProcessRuleDimension_View	This view represents MOM rules.
SC_ProcessRuleMembershipFact_View	Associates a rule to the rule groups it belongs to.
SC_ProcessRuleToConfigurationGroupDimension_View	Associates rule groups to management groups.
SC_ProcessRuleToScriptFact_View	Associates rules to response scripts. A rule can run multiple response scripts, and a response script can be called by more than one rule.
SC_ProviderDetailDimension_View	Represents instances of the data providers that are used by rules.
SC_RelationshipAttributeDefinitionDimension_View	Shows the relationship definitions.
SC_RelationshipDefinitionDimension_View	Represents the different relationships that exist between objects in MOM. The relationships are classified based on whether they involve containment of one object within the other, and whether one object is connected to the other through a data flow or workflow.
SC_RelationshipInstanceFact_View	Represents instances of relationships between two MOM items. The possible relationships are defined in the SC_RelationshipDefinitionDimension_ View.
SC_SampledNumericDataFact_View	Represents performance counter data that has been collected by MOM performance rules.
SC_ScriptDimension_View	Represents MOM response scripts.
SC_ScriptToConfigurationGroupDimension_View	Associates scripts to management groups.
SC_UserDimension_View	Represents user accounts.

In addition to the extensive System Center SQL views in the reporting database, the database includes MOM SDK SQL views to enable migrating applications from MOM 2000 SP1. These views also provide interoperability with applications that might access both operational data in the operations database and archival data in the reporting database.

APPENDIX E

Reference URLs

IN THIS APPENDIX

This appendix includes a number of reference URLs associated with Operations Manager. These links are also available "live" on the CD included with this book. URLs do change—although the authors have made every effort to verify the references here as working links, we cannot guarantee they will remain current.

You may notice that many references to pages on Microsoft's website use a "fwlink" format. Microsoft uses *fwlink* as soft or virtual links, which are pointers to specific pages. The virtual links are updated as the location of the base page changes. Using fwlinks offers a better chance of having working links.

General Resources

A number of websites provide excellent resources for Microsoft Operations Manager 2005.

- MYITFORUM.com—The myITforum.com (http://myitforum.com) site is a fantastic knowledge and information forum for those focusing on operations and systems management. MyITforum is maintained by Rod Trent, management guru extraordinaire.
- FAQShop.com—FAQShop.com provides hints, tips, and answers to Frequently Asked Questions (FAQs) relating to Microsoft systems management technologies including Microsoft Systems Management Server (SMS), Operations Manager (MOM), and Windows Software Update Services (WSUS). MOM 2005 information is available at http://www.faqshop.com/mom2005.
- SMSMOM.com—Duncan McAlynn (formerly known as Larry Duncan) has cofounded a new "unfiltered, unbiased community that you power and preserve." The site, www.smsmom.com, is intended to focus solely on SMS and MOM issues, announcements, support, and so on.

- LearnMOM.com—A subscription-based service for video-based training relating to design, administration, customization, and troubleshooting of MOM 2005; see http://www.learnsystemsmanagement.com/t-track-mom.aspx.
- Only4Gurus.com—Created by Ramon Gonzalez, a Microsoft MVP and former Microsoft employee, this site contains links to Microsoft product information and documentation, with a section for management products including MOM, http://www.only4gurus.com/v3/ShowCat.asp?Cat=Management%20/%20Operations&PP=14.
- MOM Community—A discussion forum for MOM and SC Operations Manager related topics, http://www.momcommunity.com/. Check out all the current resources for updates to blogs, links, training resources, and so on.
- Scripting available for monitoring in MOM—The scripts here include the MOM Agent Monitor script discussed in Appendix A, "MOM Internals," http://www.gotdotnet.com/codegallery/codegallery.aspx?id=ada0df24-c103-42c0-9a70-3e805be003cd.
- Recovery Planning for SQL Server Reporting Services—http://www.sqlservercentral.com/columnists/mpearson/recoveryplanningforsqlreportingservices.asp.
- Understanding MOM Reporting Data Transfer Services—http://www.myitforum.com/articles/2/view.asp?id=8639.
- Scripts and Transact SQL queries for administration tasks, courtesy of Brian Wren from Microsoft—http://www.momresources.org/scripts-momadministration.shtml.
- Brian has also compiled a series of articles on scripting in MOM. There are four articles:

  http://www.microsoft.com/technet/scriptcenter/topics/mom/mom1.mspx

  http://www.microsoft.com/technet/scriptcenter/topics/mom/mom2.mspx

  http://www.microsoft.com/technet/scriptcenter/topics/mom/mom3.mspx

  http://www.microsoft.com/technet/scriptcenter/topics/mom/mom4.mspx

- Some Microsoft blogs

  This particular blog is actually maintained by the MOM product team: http://blogs.technet.com/momteam.

  A blog by Justin Incarnato, a MOM Team Program Manager: http://blogs.msdn.com/incarnato/.

  Here's the Microsoft Product Support and Services (PSS) Manageability Official blog: http://blogs.technet.com/pssmanageability/.

- There are also blogs by several of the MOM Most Valuable Professionals (MVPs):

  Andy Dominey—http://myitforum.com/cs2/blogs/adominey/

  Blake Mengotto—http://discussitnow.spaces.live.com/

Rory McCaw—http://rorymccaw.spaces.live.com/

Justin Harter (and Pete Zerger)—http://www.momresources.org/

- Not to leave out manageability blogs by Microsoft employees:

  Steve Rachui—http://blogs.msdn.com/steverac/

  Lenny Wile—http://blogs.msdn.com/glenw/

  Clive Eastwood—http://blogs.technet.com/cliveeastwood/

  Andrzej Lipka—http://blogs.technet.com/alipka/

- Yet another blog, by Pete Zerger—http://www.it-jedi.net/
- And our own blog for MOM 2005 and Operations Manager 2007—http://ops-mgr.spaces.live.com/

Microsoft's MOM Resources

The following list includes some general Microsoft resources available for MOM 2005:

- Management Pack Catalog—This page contains descriptions and links to software used to optimize MOM. It includes links to downloadable management packs and connector software provided by Microsoft and third-party vendors. The site is continually being updated as new management packs are made available: http://go.microsoft.com/fwlink/?linkid=43970.
- MOM Product Connector Catalog—Contains links to connector software provided by Microsoft and third-party vendors http://www.microsoft.com/management/momprodconnectors.mspx.
- Its always useful to understand the licensing information about MOM—The MOM 2005 Standard Operations Management License information is available at http://www.microsoft.com/mom/howtobuy/momstdoml.mspx.
- MOM 2005 Technical Walkthroughs—Download training modules for MOM 2005 and MOM 2005 Workgroup Edition covering architecture, planning, deployment, administration, and operations at http://www.microsoft.com/downloads/details.aspx?FamilyId=2E6DF7CE-B591-4B65-B2A6-A943899B246C&displaylang=en.
- MOM Newsgroups—Microsoft maintains a number of public newsgroups for MOM for exchanging ideas and discussing common issues. See what is available at http://www.microsoft.com/technet/community/newsgroups/server/mom.mspx. Some of the more interesting ones include:

  microsoft.public.mom

  microsoft.public.mom.managementpack

  microsoft.public.mom.managementpack.ad

  microsoft.public.mom.managementpack.exchange

microsoft.public.mom.managementpack.iis

microsoft.public.mom.managementpack.sql

Links to all of Microsoft's newsgroups are available from http://www.microsoft.com/communities/newsgroups/default.mspx.

- MOM for Beginners—If you are new to MOM, it can be overwhelming to find the best information to learn how you can benefit from MOM 2005. Use this page as a reference guide to get started: http://www.microsoft.com/Mom/techinfo/training/getstarted.mspx. The web page contains links to other sites, including WebCasts.
- MOM 2005 Product Documentation—Collection of documentation covering planning and deployment, administration, security, and the Management Pack Guides accessible at http://www.microsoft.com/mom/techinfo/productdoc/default.mspx.
- MOM 2005 Frequently Asked Questions (FAQs)—http://www.microsoft.com/mom/evaluation/faqs/default.mspx.
- MOM 2005 Reviewer's Guide—http://www.microsoft.com/mom/evaluation/reviewers/default.mspx.
- MOM 2005 Security Guide—http://www.microsoft.com/technet/prodtechnol/mom/mom2005/secguide.mspx.
- MOM 2005 Management Pack Development Guide—http://go.microsoft.com/fwlink/?linkid=50020.
- MOM 2005 Conceptual Guide—http://www.microsoft.com/downloads/details.aspx?FamilyID=e06970bb-02f9-40da-b986-00d98d595696&displaylang=en.
- MOM 2005 Operations Guide—http://www.microsoft.com/downloads/details.aspx?FamilyId=A0E40758-CAB8-4588-B0F2-1508D84906CC&displaylang=en.
- MOM 2005 Deployment Planning Guide—http://www.microsoft.com/downloads/details.aspx?familyid=F3D68268-DF08-431B-8D0D-2D184E81E161&displaylang=en.
- MOM 2005 Software Development Kit—http://go.microsoft.com/fwlink/?linkid=50272.
- MOM 2005 Performance and Sizing Whitepaper—http://go.microsoft.com/fwlink/?linkid=47141.
- Authoring MOM Reports—http://www.microsoft.com/technet/prodtechnol/mom/mom2005/Library/082f04c1-b1de-4ea3-b8ce-9a6799f206e8.mspx?mfr=true.
- Information on Microsoft System Center products, including MOM 2005—http://www.microsoft.com/systemcenter/.
- Registering for Microsoft events—http://www.microsoft.com/events/inperson/. This site includes TechNet WebCasts from previous events. Some of the available WebCasts include:

Customizing Management Packs for MOM 2005—https://msevents.microsoft.com/cui/WebCastEventDetails.aspx?EventID=1032269922&EventCategory=3&culture=en-US&CountryCode=US (Chris Hallum).

Advanced MOM 2005 Reporting—https://msevents.microsoft.com/cui/WebCastEventDetails.aspx?EventID=1032263506&EventCategory=3&culture=en-US&CountryCode=US (Tom Theiner).

Managing Exchange 2003 with MOM 2005—https://msevents.microsoft.com/cui/WebCastEventDetails.aspx?EventID=1032269974&EventCategory=3&culture=en-US&CountryCode=US (Dale Koetke).

MCF and the MOM SDK—https://msevents.microsoft.com/cui/WebCastEventDetails.aspx?EventID=1032264023&EventCategory=3&culture=en-US&CountryCode=US (Vladimir Joanovic).

- MOM 2005 Resource Kit—http://go.microsoft.com/fwlink/?linkid=34629.
- Description of many of the Resource Kit utilities and components— http://www.microsoft.com/technet/technetmag/issues/2006/09/EssentialTools/default.aspx.
- MOM 2005 Deployment Guide—http://www.microsoft.com/downloads/details.aspx?familyid=03594dca-da65-44eb-875f-0ab4928cbfbd&displaylang=en.
- MOM 2005 Supported Configurations—http://www.microsoft.com/technet/prodtechnol/mom/mom2005/supconfigs.mspx.
- MOM Scripting Center—http://www.microsoft.com/technet/scriptcenter/hubs/mom.mspx.
- Understand how to monitor WMI Events— http://www.microsoft.com/technet/technetmag/issues/2006/09/WMIEvents/default.aspx.
- A Microsoft approach to using MOM for monitoring Security Events— http://www.microsoft.com/technet/technetmag/issues/2006/09/SecurityEvents/.
- MOM 2005 WebCast Series—http://www.microsoft.com/mom/support/10webcasts.mspx.
- Managing Messaging at Microsoft—http://www.microsoft.com/technet/itsolutions/msit/operations/monittsb.mspx.
- Virtual Lab for Microsoft Operations Manager 2005—http://www.microsoft.com/technet/traincert/virtuallab/mom.mspx.
- Log a bug or provide feedback to the MOM product team (requires signing into Microsoft Connect)—https://connect.microsoft.com/feedback/CreateFeedback.aspx?SiteID=209&wa=wsignin1.0.
- Report an inaccuracy on Microsoft's MOM page—Send email to momdocs@microsoft.com.

Links to Hardware Management Packs

Several of the third-party hardware management packs discussed in Chapter 19, "Interoperability," do not have online links at Microsoft's Management Pack and Product Connector Catalog; we include them on the CD to save you from having to type them in:

- IBM management pack installation process—http://publib.boulder.ibm.com/infocenter/eserver/v1r2/index.jsp?topic=/diricinfo/fqm0_t_installing_ibm_director_uim_for_mom.html.
- Information on IBM management pack—http://www-03.ibm.com/servers/eserver/xseries/systems_management/ibm_director/upward/features/mom.html
- Fujitsu management pack information—http://manuals.fujitsu-siemens.com/serverbooks/content/manuals/english/sv_integration-e.pdf.
- Unisys ES7000 Series management pack— http://www.unisys.com/products/enterprise__servers/high_d_end__servers/system__software/unisys__server__sentinel/mom.htm.

Troubleshooting

We have collected a number of troubleshooting focused references:

- RSS Feed for the most recent MOM Knowledge Base articles—http://support.microsoft.com/common/rss.aspx?rssid=2548&ln=en-us
- Log a MOM bug at—https://connect.microsoft.com/feedback/CreateFeedbackForm.aspx?FeedbackFormConfigurationID=698&FeedbackType=1&SiteID=209

Windows 2003 SP1–Related Issues

Microsoft Knowledge Base (KB) article 898921 summarizes issues that you may experience when you run the base version of MOM 2005 on a computer with Windows Server 2003 SP1; see http://support.microsoft.com/kb/898921/.

Other KB articles specific to Windows Server 2003 SP1 and MOM 2005 include

- 896989—You receive a "0x800706be" error message when you try to view the Computer Groups container in the MOM 2005 Administrator console; see article http://support.microsoft.com/kb/896989/ for details.
- 896861—You receive HTTP error 401.1 when you browse a website using Integrated Security, documented at http://support.microsoft.com/kb/896861/.
- 895952—You receive a "You do not have the appropriate privilege" error message (http://support.microsoft.com/kb/895952/).
- 895951—You receive an "UnauthorizedAccessException" error message when the MOM-to-MOM Product Connector tries to forward alert and discovery information; see http://support.microsoft.com/kb/895951/.

- 895195—You receive an "Access is denied" error message when you use the Install Agent Wizard (http://support.microsoft.com/kb/895195/).

Keep in mind that the majority of Windows 2003 SP1–related issues are resolved with installing MOM 2005 SP1.

SQL Server 2005 Required Hotfixes for MOM 2005 SP1

Three hotfixes are required to make MOM 2005 SP1 work with SQL Server 2005 for the Operational and Reporting databases. You can read the summary article at http://support.microsoft.com/kb/917615/. The individual hotfixes are located at

- Unable to discover computers in AD after upgrading to .NET Framework 2.0 (KB913812)—http://www.microsoft.com/downloads/details.aspx?FamilyId=F53F1EF3-A7A0-4C45-AEFC-7C1EC5DCCAA6&displaylang=en.
- Errors can occur when data collected by MOM 2005 SP1 is queried with SQL Server 2005 Reporting Services (KB915785)—http://www.microsoft.com/downloads/details.aspx?FamilyId=E5FC1871-1286-461D-BFCD-D32CF426E8C3&displaylang=en.
- Deadlocks may occur on SQL 2005 (KB913801)—http://www.microsoft.com/downloads/details.aspx?FamilyId=596710CC-CF17-476F-A30C-8973612F4AC7&displaylang=en.

MOM Reporting

There are several issues regarding MOM Reporting:

- Unable to import reports when using MOM 2005 SP1 and SQL Server 2005 Reporting Services. This is only an issue if you installed MOM 2005 SP1 and SQL 2005 rather than upgrading to SQL 2005 and had not already imported these management packs. The problem is documented in KB919598, at http://support.microsoft.com/kb/919598/.

  Fixes can be downloaded from http://www.microsoft.com/downloads/results.aspx?DisplayLang=en&nr=20&freetext=Operations+Manager&sortCriteria=date or by searching the management pack catalog for the most recent version of each management pack. (An update to the Virtual Server R2 management pack was not available at the time this appendix was written.) The impacted management packs include:

  Windows File Replication Services Management Pack

  Windows Terminal Services Management Pack

  Exchange Server Best Practices Analyzer Management Pack

  Windows Print Service Management Pack

  Application Center Management Pack

  Web Site and Services Management Pack

Windows DHCP Management Pack

Windows Distributed File System Management Pack

Virtual Server 2005 R2 Management Pack

- Troubleshooting MOM Reporting—http://www.microsoft.com/technet/prodtechnol/mom/mom2005/Library/1974b378-ddbb-4cbc-9f42-6d5bfb3e6d3f.mspx?mfr=true.

Heartbeat Issues

There are several known issues regarding the heartbeat:

- 892920—Agents frequently fail over to another MOM 2005 Management Server (fixed with MOM 2005 SP1), http://support.microsoft.com/kb/892920/.
- 889071—Agent alerts are not processed when Ignore Missing Heartbeats option enabled (fixed with MOM 2005 SP1), http://support.microsoft.com/kb/889071/.
- 891200—State of agent does not change after resolving all alerts (hotfix available) http://support.microsoft.com/kb/891200/.

Exchange Management Pack Issues

A number of issues related to the Exchange Management Pack were fixed with an update to the management pack, released in November 2005 (version 06.5.7719). Some outstanding issues are referred to here:

- 901050—Top 100 Mailboxes by Message Count and Top 100 Mailboxes by size reports may contain incorrect data after installing the Exchange Management Pack and Reports Option for MOM 2005, documented at http://support.microsoft.com/kb/901050/.
- 897216—TechNet Support WebCast on Troubleshooting Microsoft Exchange Management Pack for MOM 2005, discussed at http://support.microsoft.com/kb/897216/. The WebCast discusses some of the common issues and the troubleshooting steps to resolve those issues when using the Microsoft Exchange Management Pack for Microsoft Operations Manager (MOM) 2005. It also covers some best practices to use with the Exchange Management Pack for MOM.
- 891602—You receive many error alerts after you import the Exchange Server Management Pack, http://support.microsoft.com/kb/891602/.
- 890982—The MOM Exchange Management Pack Configuration Wizard may stop responding; see http://support.microsoft.com/kb/890982/.
- 886690—Exchange 2003 Management Pack Configuration Wizard crashes when the "Message Tracking" option is turned on, documented at (fixed with latest version of Wizard) http://support.microsoft.com/kb/886690/.
- 885733—Script error messages may appear repeatedly after you import and deploy the Exchange Management Pack, http://support.microsoft.com/kb/885733/.

- 835763—IADs::Put/PutEx or IADsPropertyList::PutPropertyItem calls do not accumulate; see http://support.microsoft.com/kb/835763/ for information on hotfix.

Availability Reporting Management Pack Issues

Justin Harter provides steps you can take to get the Availability Reporting Management Pack reports functional. The information is available at http://jharter.spaces.live.com/blog/cns!39CE28DB5474A6C7!264.entry.

Operations Manager 2007 and System Center Essentials

Here are some early references and articles regarding the next versions of Microsoft's Operation Management tools:

- One scenario for System Center Essentials is as a means for managing and monitoring assets of small organizations, tied to a centralized Operations Manager server. Read John Joyner's take on Microsoft's direction for management tools in the midsized market at http://www.thechannelinsider.com/article/Partners+Picture+SMB+Uses+for+Microsofts+SCE/167994_1.aspx and http://www.eweek.com/article2/0,1895,1905780,00.asp.
- Read about the System Center Roadmap (always subject to change!) at http://www.entmag.com/news/article.asp?EditorialsID=7382.
- Microsoft System Center announcements and DSI information as of May, 2006, http://www.computerworld.com.au/index.php/id;83644086;relcomp;1.
- Ongoing discussion forum for Operations Manager 2007, http://www.momcommunity.com/ShowForum.aspx?ForumID=16.
- What's new in Operations Manager 2007 (beta 2), http://blogs.msdn.com/incarnato/archive/2006/06/06/619420.aspx.
- Stewart Cawthray's review of SCOM 2007 in September 2007 issue of TechNet Magazine, http://www.microsoft.com/technet/technetmag/issues/2006/09/BetaBox/. Stewart is a Product Manager in the Windows Enterprise Division at Microsoft.
- Download the most recent version of the Beta bits at http://www.microsoft.com/mom/.
- A blog by Jakub Olesky, an SCOM developer, on Programming with System Center Operations Manager at http://blogs.msdn.com/jakuboleksy/.
- Some early blogs on System Center Essentials (SCE) are at

  http://blogs.technet.com/caseymck/

  http://blogs.technet.com/dustinj/

http://blogs.technet.com/rtammana/

http://sce.editme.com/

- Can't talk about SCE without thinking about WSUS—see the WSUS 3.0 blog at http://msmvps.com/blogs/athif/.
- Introducing System Center's "Service Desk" at http://searchwinit.techtarget.com/originalContent/0,289142,sid1_gci1184995,00.html and http://www.eweek.com/article2/0,1759,1954020,00.asp?kc=EWRSS03119TX1K0000594.

APPENDIX F

On the CD

IN THIS APPENDIX

A CD-ROM is included with this book to provide add-on value to readers of *Microsoft Operations Manager 2005 Unleashed*. Note that the authors and publisher do not guarantee or provide technical support for its contents.

Available Elsewhere

The following content can be accessed from sources other than this CD:

- MOM 2005 Sizer (Microsoft)
- MOM 2005 Resource Kit (Microsoft)
- MOM Agent Monitor (Gerald Mims)—MOM tests for agents being "alive" by checking for regular heartbeats. However, there have been times when a heartbeating agent does not send monitoring information to its management server. The Agent Monitor Management Pack tests the end-to-end functionality on the MOM agents by writing events at each agent and waiting for them to be received by the management server. (This management pack is available from www.gotdotnet.com and referenced in Appendix E, "Reference URLs.")

Only with This Book

We include an extensive list of management packs, scripts, and references, available only with the book:

- Backup script management pack with script for files used by MOM—Automates the process of backing up databases, management pack and report source files, and other customized files used by MOM. To be customized for your particular environment. The script and management pack is described in Chapter 11, "Backup and Recovery."

MORE ABOUT DATABASE BACKUPS

Most MOM installations do not use named database instances for the operational and reporting databases. The backup script as written supports backing up databases on the default instance only.

If your MOM environment uses named instances, you can modify the script by adding the instance information as illustrated below, changing *instancename* to the name of your database instance. This particular example backs up the OnePoint database:

The line in the script

```
osql -S %computername% -E -Q "BACKUP DATABASE OnePoint TO DISK =
'%backup%\onepoint.bak' WITH INIT, NAME = 'onepoint.bak'"
```

Needs to be changed to

```
osql -S %computername%\instancename -E -Q "BACKUP DATABASE OnePoint TO DISK
= '%backup%\onepoint.bak' WITH INIT, NAME = 'onepoint.bak'"
```

This change needs to be made for all databases on the server where the named instance is implemented, such as the management server, reporting database server, and/or SSRS server."

- Escalation Notification Management Pack—(Basic) escalation alerting of unresolved alerts in MOM. When alerts are left open, notifications are sent to responsible parties specified in MOM's notification groups. This management pack is introduced in Chapter 14, "Monitoring with MOM."
- Maintenance Mode Management Pack—Automates the process of putting computers into maintenance mode, invoking the mominfo.exe program in the MOM 2005 Resource Kit. The maintenance mode MP is discussed in Chapter 14.
- Monitoring Drives for Free Space—Modified version of Microsoft's Windows Storage State Monitoring script (part of the Base OS Management Pack). Sometimes you have specific drives that have limited free space, which is okay and actually does not indicate a problem. The script modifications allow you to modify the management pack to exclude a specific drive from being monitored for free space. This script is discussed in Chapter 15, "Managing the Operating System."
- Monitoring the MOM database—Tracks and reports on database size and growth statistics for the MOM operational and reporting databases. This is something every installation wants, and Microsoft doesn't provide! We include documentation, management pack rules and MOM reports. The Database Tracking management pack is in a self-extracting zip file and introduced in Chapter 18, "Database Management."

- SecurityPack—Monitors security events on domain controllers including failed logon attempts, changes to administrative group membership, and events associated with user account management. This management pack is included with a discussion of creating your own management packs in Chapter 20, "Developing Management Packs."
- PingPack—Provides notifications (alerts) when non-Microsoft systems are unavailable. It determines whether an IP-based device is online and responding to a Ping. We include several rules and scripts as part of the PingPack and use it as an example of developing your own management pack. This type of functionality is available from third-party vendors as a chargeable item; we include our version with the book. Detailed steps on creating the PingPack are included with Chapter 20.
- Network System Monitoring Pack—Enhances the PingPack, adding parameter support, a WMI ping, performance counters, and state variables. This management pack is discussed in Chapter 20.
- Reference URLs (Appendix E)—Included as Live Links, more than 100 (clickable) hypertext links and references to materials and sites related to Operations Manager.

  A disclaimer and unpleasant fact regarding live links—*URLs change*. Companies are subject to mergers and acquisitions, pages move and change on websites, and so on. Although these links were accurate in mid-2006, it is possible some will change or be "dead" by the time you read this book. Sometimes the Wayback Machine (http://www.archive.org/index.php) can rescue you from dead or broken links. This site is an Internet archive, and will take you back to an archived version of a site… sometimes.

This page intentionally left blank

Symbols

A

B

C

D

E

F

G

H

I

J

K–L

M

N

O

P

Q

R

S

T

U

V

W–Z