

Kerrie Meyler  
Cameron Fuller  
John Joyner



with Andy Dominey

# System Center Operations Manager 2007

**UNLEASHED**

**SAMS**

## System Center Operations Manager 2007 Unleashed

Copyright © 2008 by Sams Publishing

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-672-32955-7

ISBN-10: 0-672-32955-7

*Library of Congress Cataloging-in-Publication Data:*

Meyler, Kerrie.

System center operations manager 2007 unleashed / Kerrie Meyler, Cameron Fuller, John Joyner ; with Andy Dominey.

p. cm.

Includes bibliographical references and index.

ISBN 0-672-32955-7 (alk. paper)

1. Electronic data processing—Management. 2. Computer systems—Evaluation. 3. Computer networks—Management. 4. Microsoft Windows server. I. Fuller, Cameron. II. Joyner, John. III. Dominey, Andy. IV. Title.

QA76.9.M3M59 2008

005.4'476—dc22

2008000571

Printed in the United States on America

First Printing February 2008

### Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Sams Publishing cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

### Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the CD or programs accompanying it.

### 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**

**Editor-in-Chief**  
Karen Gettman

**Executive Editor**  
Neil Rowe

**Development Editor**  
Mark Renfrow

**Managing Editor**  
Gina Kanouse

**Senior Project Editor**  
Lori Lyons

**Copy Editor**  
Bart Reed

**Indexer**  
Cheryl Lenser

**Proofreader**  
Lisa Stumpf

**Technical Editors**  
Kevin Saye,  
Brett Bennett

**Publishing  
Coordinator**  
Cindy Teeters

**Multimedia Developer**  
Dan Scherf

**Book Designer**  
Gary Adair

**Composition**  
Jake McFarland

**Manufacturing Buyer**  
Dan Uhrig



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.sampublishing.com/safarienabled>
- ▶ Complete the brief registration form
- ▶ Enter the coupon code XELV-7D4M-5ES2-RXM6-HBNE

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

# Introduction

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.

With System Center Operations Manager 2007, Microsoft continues its commitment to providing a solid monitoring and management product. Although Microsoft licensed NetIQ's Operation Manager technology in 2000, not until Operations Manager 2007 did Microsoft put its finishing touches on reengineering the product. Now in its third major release, the software formerly known as "MOM," or Microsoft Operations Manager, has been rewritten and rebranded into Microsoft's System Center product line. Operations Manager 2007 concentrates on end-to-end application monitoring, moving beyond its previous server monitoring focus.

Operations Manager 2007 monitors the health of an application, defined and measured by the health of the various pieces that make up that application. In today's environment, applications are no longer monolithic, so monitoring health typically includes network devices and the various pieces of a distributed application. Monitoring at the component level means that if a database used by an application has a problem, Operations Manager knows which application is affected.

Operations Manager 2007 also brings to the plate the capability to manage security and audit data, client machines,

and common desktop applications, and collect and report on user application errors. Rather than being evolutionary in its changes as are most version updates to an application, Operations Manager 2007 is truly revolutionary in its approach to monitoring when compared to its MOM 2005 predecessor.

Successfully implementing Operations Manager requires planning, design, and a thorough understanding of how to utilize its many capabilities. This complete guide for using Operations Manager 2007 from the authors of *Microsoft Operations Manager 2005 Unleashed* gives system administrators the information they need to know about Operations Manager 2007 and what it can do for their operations—from an overview of why operations management is important, to planning, installing, and implementing Operations Manager 2007.

*Microsoft System Center Operations Manager 2007 Unleashed* provides a comprehensive guide to this newest version of Microsoft's premier management product.

As always, we do have a disclaimer: Resources and management packs related to the product continue to change rapidly. Sometimes it seemed that even before we finished a chapter, the information was changing. This has been particularly challenging because Microsoft is close to releasing its first service pack for Operations Manager 2007 as we complete this book. We have done our best to present the information as it relates to both the released version and the service pack, even as that continues to take shape. The information in the 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, utilities, URLs, and Knowledge Base articles.

## Part I: Operations Management Overview and Concepts

Part I of this book introduces the reader to Operations Manager 2007 (OpsMgr), outlining its features and functionality and comparing and contrasting it to MOM 2005.

- ▶ Chapter 1, “Operations Management Basics,” discusses the concepts behind operations management and Microsoft's management approach, and introduces Microsoft's management suite of products. An overview of ITIL and MOF (and an alphabet soup of other acronyms) is included, along with a discussion of how the different MOF quadrants relate to Operations Manager.
- ▶ Chapter 2, “What's New,” appropriately tells you just that. You will find there is an incredible amount of new functionality in this version! We also cover the history of Operations Manager and compare OpsMgr 2007 with MOM 2005 and System Center Essentials 2007.
- ▶ Chapter 3, “Looking Inside OpsMgr,” discusses the Operations Manager components, its processing flow and architecture, and how management packs work.

## Part II: Planning and Installation

Before diving into OpsMgr's setup program, it is best to take a step back to map out the requirements for your management environment and plan your server topology.

- ▶ Chapter 4, "Planning Your Operations Manager Deployment," discusses the steps required for successfully planning an Operations Manager installation. We also introduce the OpsMgr databases sizing spreadsheet and discuss the logic behind the sizing calculations.
- ▶ Chapter 5, "Planning Complex Configurations," addresses advanced implementations of OpsMgr. We also discuss planning for redundancy and designing large and more interesting environments.
- ▶ In Chapter 6, "Installing Operations Manager 2007," we discuss hardware and software requirements before going through the steps to install the various server components in a management group.
- ▶ Chapter 7, "Migrating to Operations Manager 2007," discusses the required steps to migrate from an existing MOM 2005 environment to OpsMgr 2007. Note that the process is a migration, not an upgrade. If you have MOM 2005, you will want to read this chapter—because not everything can be migrated.

## Part III: Moving Toward Application-Centered Management

With OpsMgr 2007 installed, how does one start using it? Part III moves beyond setup to post-installation activities and potential adjustments to your initial configuration.

- ▶ Chapter 8, "Configuring and Using Operations Manager 2007," discusses what you need to know to get started with OpsMgr. We provide an overview of the Operations console and a drilldown into its functionality.
- ▶ Chapter 9, "Installing and Configuring Agents," goes through the details of computer discovery, the different techniques for implementing agents, and potential problems related to agent installation.
- ▶ Chapter 10, "Complex Configurations," discusses various management server and management group configurations, and presents suggestions for implementing redundant components.
- ▶ In Chapter 11, "Securing Operations Manager 2007," we discuss role-based security, Run As Profiles and Accounts, required accounts, and mutual authentication, as well as when you need and how to install certificates. We also discuss security for the ACS component, an optional but highly recommended part of your OpsMgr implementation.

## Part IV: Administering Operations Manager 2007

All applications require administration, and OpsMgr is no exception.

- ▶ Chapter 12, “Backup and Recovery,” discusses the components required for a complete backup and recovery plan, and the steps for designing 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 converting, importing, and exporting management packs into your OpsMgr environment.
- ▶ Chapter 14, “Monitoring with Operations Manager,” discusses the different monitors and rule types in Operations Manager and their functionality. It also covers creating alerts, overrides, resolution states, notification workflow, and approaches for tuning monitors and rules.

## Part V: Service-Oriented Monitoring

In this section of the book we get into what Operations Manager 2007 is really about—using it to ease the pain of monitoring and managing your environment, from end-to-end. We discuss using OpsMgr to manage different aspects of your environment.

- ▶ Chapter 15, “Monitoring Audit Collection Services,” focuses on auditing and security monitoring concerns. Audit Collection Services is a new component with OpsMgr 2007 that is a valuable addition to your monitoring toolkit.
- ▶ In Chapter 16, “Client Monitoring,” we discuss new capabilities in OpsMgr for client monitoring. We also cover managing crash errors using the new Agentless Exception Monitoring functionality.
- ▶ Chapter 17, “Monitoring Network Devices,” shows how to use Simple Network Management Protocol (SNMP) with OpsMgr and discusses monitoring hardware and network devices.
- ▶ Chapter 18, “Using Synthetic Transactions,” talks about simulating connections into applications to verify their performance.
- ▶ Chapter 19, “Managing a Distributed Environment,” discusses OpsMgr’s capability to monitor the various pieces and components that make up the distributed applications commonly used in today’s multisystem computing environment.

These chapters talk about the issues faced by administrators in each of these areas, and they show how Operations Manager 2007 helps to monitor operational issues and maintain application health and stability.

## Part VI: Beyond Operations Manager

In this section we look at extending one's use of Operations Manager 2007 with connectors, third-party management packs, and customization. We also look at Microsoft's direction for operations management.

- ▶ Chapter 20, "Automatically Adapting Your Environment," begins the last part of the book by looking at how you can use Operations Manager 2007 to automatically adapt your environment as changes occur.
- ▶ Chapter 21, "Reading for the Service Provider: Remote Operations Manager," talks about utilizing OpsMgr 2007 in conjunction with System Center Essentials 2007 in Microsoft's hybrid product designed for use by service providers.
- ▶ In Chapter 22, "Interoperability," we cover connecting to other management groups, the role of product connectors in communicating with other management systems and third-party enterprise consoles, and integration between OpsMgr 2007 and other System Center components. This chapter also discusses management packs that monitor hardware, other operating systems, and network components.
- ▶ Chapter 23, "Developing Management Packs and Reports," discusses the process of customizing OpsMgr using management packs and reports. Although XML plays a big part in this, we also discuss other tools, including the part the Authoring and Operations consoles play in developing management packs.

## Appendixes

This book contains six appendixes:

- ▶ Appendix A, "OpsMgr by Example: Configuring and Tuning Management Packs," is a compilation of articles from the *OpsMgr by Example* series published in our Operations Manager blog (<http://ops-mgr.spaces.live.com>).
- ▶ Appendix B, "Performance Counters," discusses the performance counters specific to Operations Manager.
- ▶ Appendix C, "Registry Settings," discusses some of the more significant Registry settings used by Operations Manager 2007.
- ▶ Appendix D, "Active Directory and Exchange 2003 Management Pack Parameters," lists parameters for shared scripts in the Active Directory (AD) and Exchange 2003 management packs.
- ▶ Appendix E, "Reference URLs," provides references and descriptions for many URLs helpful for OpsMgr administrators. These are also included on the CD as live links.
- ▶ Appendix F, "On the CD," discusses the utilities on the CD accompanying this book.

## Conventions Used in This Book

Here's a quick look at a few book elements designed to help you get the most out of this book:

Text that you are supposed to type is styled in bold type, as in the following examples:

In the Properties dialog, enter **Agent View** in the Name field.

Open the Operations Manager command shell and enter the following command:

**C:\DumpMPContents.ps1 -mpDisplayName:'<management pack name>'**

When a line of code is too long to fit on only one line of this book, it is broken at a convenient place and continued to the next line. The continuation of the line is preceded by a code continuation character (►). You should type a line of code that has this character as one long line without breaking it.

### NOTE

#### For Extra Information

The Note box presents asides that give you more information about the current topic. These tidbits provide extra insights that give you a better understanding of the task. In many cases, they refer you to other sections of the book for more information.

### TIP

#### Quick Ideas

Tips point out quick ways to get the job done, or good ideas or techniques.

### CAUTION

#### Important Information

Cautions contain warnings or significant material about potential pitfalls, including information critical to the proper functioning of your system.

## About the CD

This book includes a CD containing scripts, utilities, and examples 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 and strange-looking URLs. The Operations Manager 2007 Resource Kit (Wave 1) is also on the CD.



## Who Should Read This Book

This book is targeted towards systems professionals who want to be proactive in managing their operational environments. This book is targeted toward systems professionals who want to be proactive in managing their operational environments. These individuals are responsible for the operational health of the operating system and the subsystems running within it. This book should be a useful tool for system administrators regardless of the size of their organization or the industry in which it resides. By providing insight into Operation Manager's many capabilities, discussing tools to help with a successful implementation, and sharing real-world experiences, we hope to enable a more widespread understanding and use of System Center Operations Manager.

## CHAPTER 3

# Looking Inside OpsMgr

Microsoft System Center Operations Manager 2007 (OpsMgr) is a monitoring and operations management system, implemented using one or more computers that perform their assigned roles as components of a management group. The components cooperate over several secure communication channels to achieve management information workflow and present information to operators and administrators. The most important data collected is the health of the managed objects; this health status is arrived at via models that affect the tactical placement of software probes called *monitors*.

This chapter endeavors to make these terms and relationships clear so that the job of deploying and supporting OpsMgr 2007 becomes easier and more effective. Those readers tempted to skip this chapter covering OpsMgr internals, definitions, and concepts are probably asking themselves, “What practical use can I expect to get from reading this chapter?” Some administrators avoid looking under the hood deliberately, and that’s totally OK. For those individuals, we do recommend reading at least the “Management Group Defined” section of this chapter.

So, for those OpsMgr administrators who yearn to know exactly what is going on behind the scenes, this chapter is for you. We want you to understand the lingo and reasoning used by the software developers of Operations Manager. In doing so, we hope that more advanced material about OpsMgr will make sense more quickly to you, the OpsMgr administrator, when reading this book, using the product, or interacting with fellow professionals in the Microsoft systems management community.

### IN THIS CHAPTER

- ▶ Architectural Overview
- ▶ Windows Services
- ▶ Communications
- ▶ How Does OpsMgr Do It?
- ▶ Presentation Layer

## Architectural Overview

This chapter looks at OpsMgr design and internals at two levels:

- ▶ **The macro level**—We'll look at the computer roles that comprise a management group.
- ▶ **The micro level**—We'll examine the objects that constitute a management pack, in particular its workflow and presentation of data to the operator.

As an OpsMgr administrator, you have no influence over server component characteristics—these are hard-coded features of the Operations Manager software and hardware architecture. On the other hand, administrators can enjoy almost complete flexibility regarding the manner in which management packs are utilized.

OpsMgr administrators of the smallest environments—administrators who will run all applicable OpsMgr components on a single server and manage only computers and devices on their local area network (LAN)—generally are less concerned about this section on OpsMgr architecture. In that small-scale scenario of the “all-in-one” management group server, there is much less to be concerned about with architectural considerations of the various OpsMgr computer roles (components) as long as you stay below capacity thresholds for that single server and its network segment. In this simplest OpsMgr environment, the only OpsMgr components not resident on the single server are the OpsMgr agents running on the managed computers on the network.

However, many OpsMgr administrators will need to distribute multiple components across different servers, deploying OpsMgr roles across multiple computers. Even OpsMgr 2007 deployments on small business networks may include an Audit Collection Services (ACS) Component to centralize security event auditing, or an OpsMgr Gateway Server Component to monitor service delivery at a branch office where there is no Virtual Private Network (VPN) connectivity. Deploying the feature sets added when installing these additional roles, by definition, adds one or more physical management servers to the management group and requires an understanding of Operations Manager 2007 management group architecture. Chapter 4, “Planning Your Operations Manager Deployment,” and Chapter 5, “Planning Complex Configurations,” provide information on hardware specifications and sizing server configurations.

### Management Group Defined

A *management group* is an instance of the Microsoft end-to-end service management solution named Operations Manager 2007. Organizations may host several management groups (instances of OpsMgr on their networks) if appropriate for their business needs. Likewise, any managed computer or device can participate in one or more instances (management groups) of OpsMgr if appropriate. Most organizations of all sizes deploy a single management group, which is analogous to a single Active Directory (AD) forest or a single Exchange organization. Most organizations, including some very large ones, have their business needs met with just one AD forest and one Exchange organization.

Figure 3.1 illustrates a default, single management group in an organization, and contrasts that with a more complex implementation one might encounter in a large organization. In the simple all-in-one example on the left in Figure 3.1, all OpsMgr components are installed on one server, which is the only OpsMgr server in the single management group serving the managed computers (agents) in the organization. Several hundred computers can be managed with an all-in-one deployment of OpsMgr 2007.

In the complex large organization scenario on the right-hand portion of Figure 3.1, a single computer agent is reporting simultaneously to two management groups (known as a *multihomed* agent), while one of those management groups, through its Root Management Server (RMS), participates with several connected management groups. This creates an architecture capable of servicing tens of thousands of widely distributed computers.

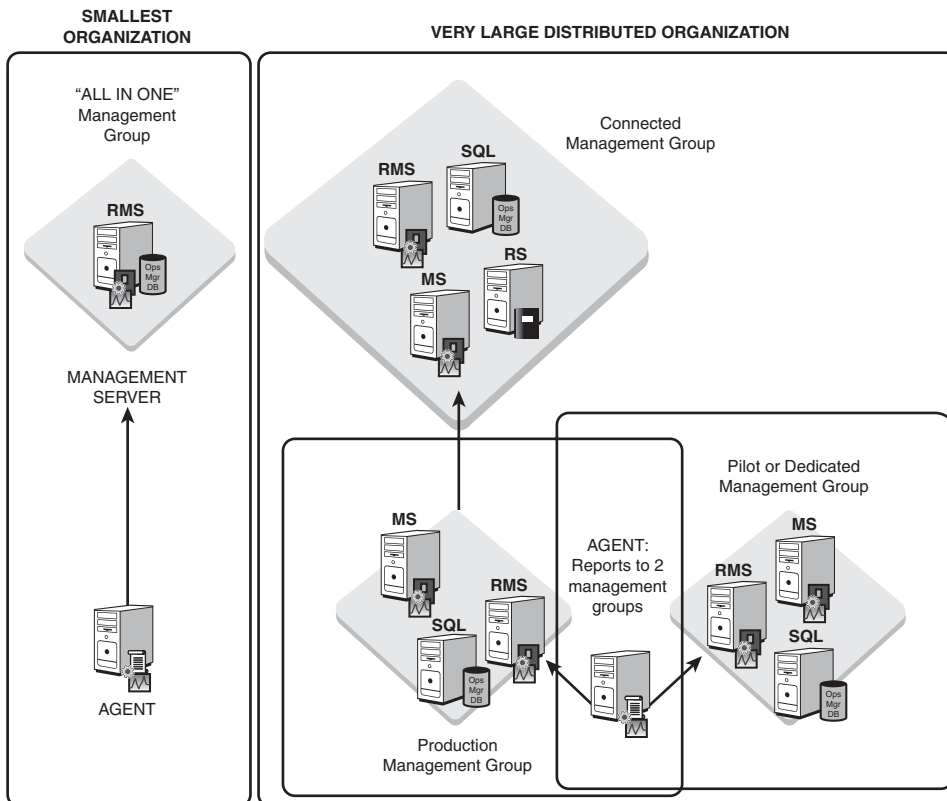


FIGURE 3.1 Contrasting the smallest with a very large OpsMgr 2007 deployment model.

You will seldom need multiple management groups to get the most out of OpsMgr 2007 since the product's design provides full functionality to all but the largest of organizations

while still using a single management group. For the very large organization (over 10,000 computers or over 100 remote sites), deploying several OpsMgr 2007 management groups can distribute the workload. Connecting these management groups enables you to query multiple management groups from the same Operations console.

Both having more than one production instance of OpsMgr in your organization and having a computer or device report status to more than one management group are advanced configurations to accomplish particular business goals. We describe these situations in Chapter 10, “Complex Configurations.”

## TIP

### Management Group Names

A management group name is a unique alphanumeric name specified by the administrator when installing the Operations Database Server Component. The management group name cannot be changed after installation, so it is a good idea to select a name that is easy to remember and makes sense given the organization’s geographic or administrative needs.

When creating a management group, remember that the name is case-sensitive.

## Server Components

Here are a dozen possible computer components, or roles, that can be deployed in an OpsMgr 2007 management group. Focusing now on what components constitute a single OpsMgr 2007 management group, let’s begin with describing the core, or basic, server components. The core components are those that an OpsMgr 2007 deployment must include to have minimum functionality. These basic components (displayed in Figure 3.2) are installed in every management group, including the all-in-one server OpsMgr environment.

- ▶ **Operations Database Server Component**—The heart of the management group is the Operations database. The Operations database contains operational data about managed objects, the configuration store of what objects are managed, and all customizations to the OpsMgr environment. The Operations database is the central repository and processing point for all data in a management group. When you install an OpsMgr 2007 management group on multiple computer systems, the first thing to take place is installing the Operations database on an existing SQL 2005 database server running Service Pack (SP) 1 or later. The Operations Database Server Component can be clustered in high-availability environments.
- ▶ **Root Management Server Component**—The first management server installed in a management group is the Root Management Server Component. Like all OpsMgr 2007 management servers, the RMS sends configuration information to managed computers and receives data from agents. The RMS alone runs some distinctive services that the entire management group depends on, and like the Operations Database Server Component, the RMS Component can be clustered. The RMS requires that the Operations database be available and accessible. The function of

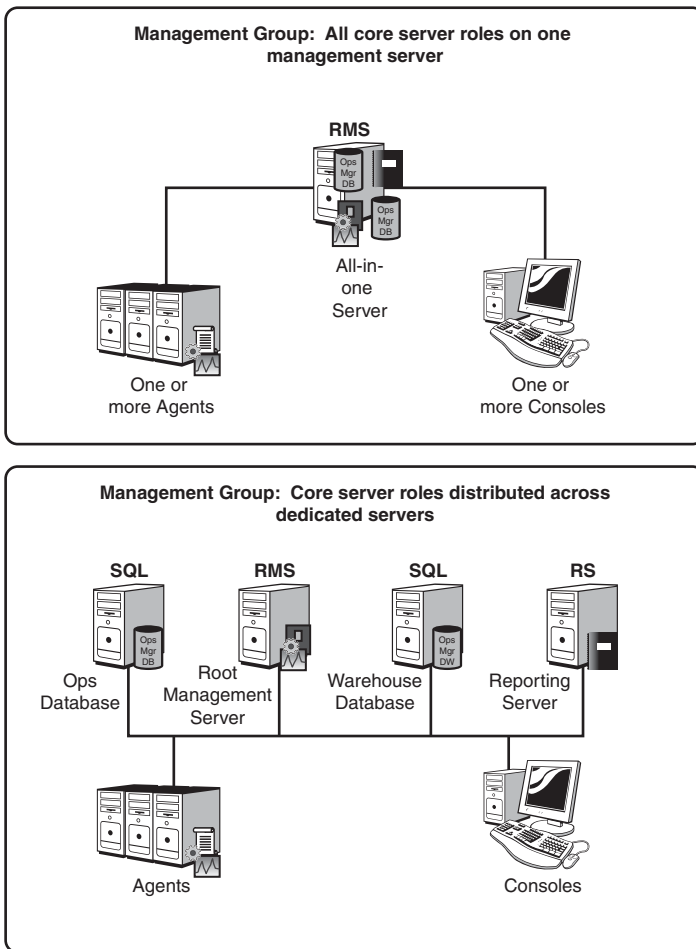


FIGURE 3.2 OpsMgr 2007 core components combined in one server, and distributed across dedicated servers.

the entire management group also depends on the RMS; in high-availability environments you should consider clustering both the Operations database and the RMS components.

- **Agent Component**—The Agent Component is used to monitor servers and clients. This is a Windows service that runs on managed servers and client computers. You might create an all-in-one server management group whose only purpose is monitoring network devices such as routers or switches; in that case, no agents need to be deployed. However, for most OpsMgr setups, the deployment of core management group components is not complete until one or more computers are selected for management and the Agent Component is installed. As we mentioned previously in

the “Management Group Defined” section of this chapter, an OpsMgr 2007 agent can participate in more than one management group simultaneously.

- **Console Component**—The OpsMgr 2007 console is the only application needed to interact with the management group, and it is used by both operators and administrators. Operations Manager 2007 implements role-based security to ensure an optimized experience for all users. There is also a web-based console with a subset of the regular console functions.

Each console connects directly to the RMS, even if additional management servers have been deployed in the management group. This dependence makes RMS availability critical to perform almost every function in OpsMgr 2007. The first time a user opens the Operations console, there is a prompt to enter the name of the RMS, unless the user accessing the console is at a management server. After connecting, the console stores that server name, as well as the management group name, in the Connect to Server dialog box shown in Figure 3.3.



FIGURE 3.3 The Connect to Server dialog box stores the name of the RMS and associated management group.

The four components listed here are mandatory components and required for any OpsMgr management group to function. In addition, there are two core components related to reporting that most OpsMgr administrators will install regardless of their environment size:

- **Reporting Data Warehouse Server Component**—A long-term data store is created with the Reporting Data Warehouse Server Component. The data warehouse stores aggregated historical performance and availability data beyond the few hours or days of data available in the Operations database. Without a data warehouse, an OpsMgr management group will only present information based on the real-time and very recent data captured in the Operations database, which is aggressively groomed of historical data. The Reporting Data Warehouse Server Component can be hosted on a clustered SQL Server backend.

- **Reporting Server Component**—This component adds the reporting function to an OpsMgr management group and is required for the Reporting Data Warehouse Server Component. The Reporting Server is installed on a server running SQL Reporting Services 2005 SP 1 or later. Because of the integration between the Operations console and the Reporting Server, it is transparent to the user that the data for the reports is coming from the Reporting Server and not the Operations database or the RMS. This differs from the Microsoft Operations Manager (MOM) 2005 Reporting implementation.

You can install the Reporting Data Warehouse Server and Reporting Server Components on the same Windows server, although in large and high-availability environments, these two components typically run on dedicated servers.

Finally, there are six optional components in an OpsMgr management group. Computers are deployed with these components as needed or desired to increase the monitoring capacity, or to add further features to the management group:

- **Management Server Component**—This component refers to additional management servers installed after the RMS is installed. The primary reasons to deploy additional OpsMgr 2007 management servers are to enable agent failover and to manage a larger number of objects. There are specific procedures to promote a management server to the RMS Role in a disaster-recovery scenario, which we discuss in Chapter 12, “Backup and Recovery.” You would also install an additional management server to host the Audit Collector Component, described later in this list, because that component requires installation on an existing OpsMgr management server that is not the RMS.
- **Audit Database Server Component**—SQL Server 2005 is required for the Audit Database Server Component when adding the Audit Collection Services feature to the management group. Security events from managed computers are stored in this database and are used in generating reports. The Audit Database Server can be a clustered service for high availability. Reports on security events are generated from the Audit database.
- **Audit Collector Component**—This server function collects events from the audit collection-enabled agents. The Audit Collector Component is added to an existing OpsMgr management server. Audit collection is enabled on OpsMgr agents by running a task in the OpsMgr console. Each collector needs its own individual Audit Database Server. The Audit database can be located on the same computer as the ACS Collector, but for optimal performance, each of these components should be installed on a dedicated server.
- **Web Console Server Component**—Any OpsMgr management server running the Internet Information Services (IIS) web server service can optionally host a web-based version of the OpsMgr console. Functionally similar to using a thin client much like Outlook Web Access (OWA), operators can view topology diagrams and



performance charts and run tasks made available to them appropriate for their role. The Web Console Server might be a management server dedicated to hosting this role in an organization that makes heavy use of the Web console.

- ▶ **Gateway Server Component**—A communications conduit to monitoring agents in untrusted domains (or on remote networks without routed network connectivity), this server resides in an external environment and uses certificates to secure communication back to the other roles in the management group. A gateway server can also host the Audit Collector Component.
- ▶ **Client Monitoring Server Component**—The Client Monitoring Configuration Wizard is used to configure the Client Monitoring Server Component on one or more management servers in a management group. The Agentless Exception Monitoring (AEM) Client Component is activated by a Group Policy Object (GPO) applied to client computers. An important note is that the management server and AEM clients must be in the same domain or fully trusted domains.

Figure 3.4 illustrates a management group with all components on distributed servers, and with many high-availability features deployed. This large-enterprise management group could provide end-to-end service monitoring of many thousands of objects with a high degree of reliability.

### Sharing Resources Between Management Groups

We have discussed how the OpsMgr agent on a managed computer can be a member of more than one management group. There are other ways to leverage hardware across multiple management groups, particularly at the database server layer. Because the Operations database can be assigned any user-selectable name during installation, and because the Data Warehouse database natively supports multiple management groups, a single SQL 2005 server can provide database backend services to multiple management groups, which need not be aware of each other.

This feature lets organizations with more than one management group consolidate OpsMgr database duties to a single SQL Server, or more likely a highly available clustered SQL Server configuration. This significantly reduces the incremental cost of adding another management group in an organization.

## Windows Services

Computers running OpsMgr components also host particular Windows services in specific configurations depending on their function(s). The presence of the OpsMgr Health service is universal to all Windows computers participating in an Operations Manager 2007 management group. The next sections describe the Health service as well as the other four services that exist in a management group with Audit Collection Services deployed.

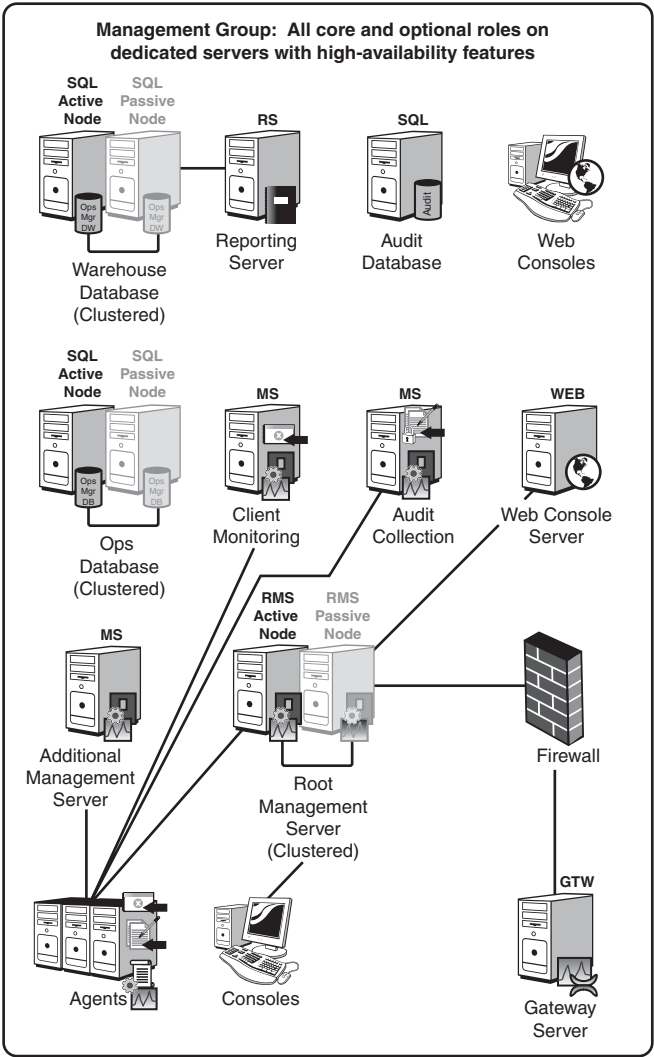


FIGURE 3.4 All basic and optional OpsMgr server roles deployed on dedicated servers.

### OpsMgr Health Service

The Health service provides a general execution environment for monitoring modules. Such modules form different workflows, enabling end-to-end monitoring scenarios.

### Health Service Implementations

There are actually two flavors of the Health service:

- ▶ The first implementation, the Agent Health service, runs on monitored Windows computers. The service executes tasks, collects performance data, and performs other functions on the managed computer. The Agent Health service continues to run, collecting data and performing tasks, even when disconnected from a management server. Data and events accumulate in a disk-based queue, and they are reported when the connection to the management server is restored.
- ▶ The other implementation of the Health service runs on a management server. The functionality of the Health service running on a management server varies depending on the setup of the management group and the management packs installed.

Installing new or additional management packs extends the Health service running on both types of computers (agent-managed computers and management servers). Another important feature of the Health service is that it provides credential management services to other OpsMgr processes, supporting execution of modules running as different users.

### Security

A public/private key pair, used for secure communications, is created on each instance of the Health service (RMS, Management Server, Gateway Server, and agent). This key pair can be regenerated at any time. The public key is published at the following times:

- ▶ During startup
- ▶ When the key expires
- ▶ During a failure to decrypt a message
- ▶ Upon request by the SDK (discussed in the next section) to republish the key

If the key is not successfully published, the SDK may post errors. The agent key may also drop “key mismatch” events. Because OpsMgr is self-healing, the agent republishes the key or the SDK re-requests the key if there is a problem. When the key is close to expiring, the Health service restarts itself, regenerating the key. If you think the key has been compromised, remove it and restart the Health service to generate a new key.

### OpsMgr SDK Service

The OpsMgr SDK service is found in the services list of all management servers. However, the service is disabled unless the server is also the RMS. This service and the OpsMgr Config service, described next, are both found only on management servers. All data flowing to and from the Operations database is transported via the OpsMgr SDK service running on the RMS.

The SDK service is responsible for providing access for the OpsMgr console to the Operations database, viewing the current state of a monitored object, importing management packs to the database, storing management packs in the database, and storing management group configuration information in the database. The SDK service also handles the following functions:

- ▶ Writing event data to the database
- ▶ Writing state-change data to the database
- ▶ Writing performance counter data to the database

In addition, the SDK service owns a symmetric encryption key for the management group that accesses the Run As Account information, which is stored in the Operations database. We introduced Run As Accounts in Chapter 2, “What’s New.”

The encryption key information is stored in the Registry. If you lose this key, you will have to clear out and reset the Run-as accounts. The management group key is also required if you are promoting a management server to become your new RMS and want to keep your Run As Accounts. You can back up and restore this key using a Microsoft-provided key backup tool. This process is further discussed in Chapter 10.

## OpsMgr Config Service

Similar to the OpsMgr SDK service described earlier, the OpsMgr Config service will also be found installed on all management servers, but disabled unless the server is also the RMS. The OpsMgr Config service manages the relationships and the topology of the OpsMgr 2007 environment.

The OpsMgr Config service is responsible for providing the monitoring configuration to each agent’s Health service, which may include sensitive information. The service acts as an intermediary for delivering sensitive information in an encrypted format from the Operations database to the target Health service on a monitored agent.

## OpsMgr Audit Forwarding Service

This service sends events to an ACS collector server for storage in a SQL Server database. The Audit Forwarding service is found on each Windows computer in an OpsMgr management group. By default, the service needed for an agent to be an ACS forwarder is installed but not enabled when the OpsMgr agent is installed. After you install the ACS collector and database, you can then remotely enable this service on multiple agents through the Operations console by running the Enable Audit Collection task.

## OpsMgr Audit Collection Service

The Audit Collection service is responsible for receiving audit events over the network and writing them to the Audit database. This service is found running on management servers that also have the ACS Audit Collector Service Component Installed. The service and the Audit database are created during setup of the ACS service on the selected management server(s).

## Communications

Operations Manager 2007 uses a variety of communications methods that are optimized for security and efficiency. Communication with the three OpsMgr database backend components—the Operations database (DB), the Data Warehouse DB, and the Audit Collection Services DB—is always via standard SQL client/server protocols, specifically OLE DB (Object Linking and Embedding Database).

Between agents, as well as management and gateway servers, the primary Transmission Control Protocol (TCP) port used by OpsMgr is 5723, which is the only outbound firewall hole needed to manage a computer in a minimal configuration (after the agent is installed or preinstalled). Additional outbound ports are used when enabling ACS and AEM. A complete list of communications protocols and default ports used in an OpsMgr management group is provided in Table 3.1.

The logic in Table 3.1 is diagrammed in Figure 3.5. A quick study of the communication paths verifies the criticality of the RMS in an OpsMgr 2007 management group. The RMS is clearly the communications nexus for the monitoring organization, with most features of OpsMgr unavailable if the RMS is down or inaccessible. Of course, the RMS depends completely on its connection to the Operations database to function.

In effect, both the RMS and the Operations database need to be continuously available to provide uninterrupted continuity of management functions. That makes clustering the Ops DB and the RMS top considerations when seeking to architect a highly available management solution for the enterprise. For computers managed via the Gateway Server Component, additional gateway servers can be deployed to the same remote domain or site, providing failover coverage to one another.

The diagram in Figure 3.5 does not illustrate the need for RPC/DCOM communication between a management server and a managed computer in order to push the agent to a managed computer. Details on this, as well as how to configure the Windows Firewall on a managed computer to perform “push” installation of the agent from a management server, are covered in Chapter 9, “Installing and Configuring Agents.”

TABLE 3.1 Communication Paths and Ports

From Component	To Component	Bidirectional	TCP Port
Root Management Server (RMS) or Management Server (MS)	Operational Database (Ops DB) and Data Warehouse Database (DW DB)	No	OLE DB 1433 (SQL); in a cluster the second node requires a unique port number.
RMS	MS or Gateway Server	Yes	5723.
Operations console Agent	RMS, MS, or Gateway	No	5723.
Reporting Server, Web Console Server	RMS	No	5724.
Connector Framework Source	RMS	No	51905.
Agentless Exception Monitoring (AEM) Client	AEM file share on RMS or MS	No	SMB 445, 51906.
Software Quality Metrics (SQM) Client	SQM Endpoint	No	51907.
Web console	Web Console Server	No	HTTP 51908.
Audit Collection Services (ACS) Agent	ACS Collector	Yes	59109.
ACS Collector	ACS DB	No	OLE DB 1433 (SQL).
Reporting Server	DW DB	No	OLE DB 1433 (SQL); in a cluster the second node requires a unique port number.
Operations console	Reporting Server	No	HTTP 80.

COMMUNICATION PATHS AND FIREWALL CONSIDERATIONS

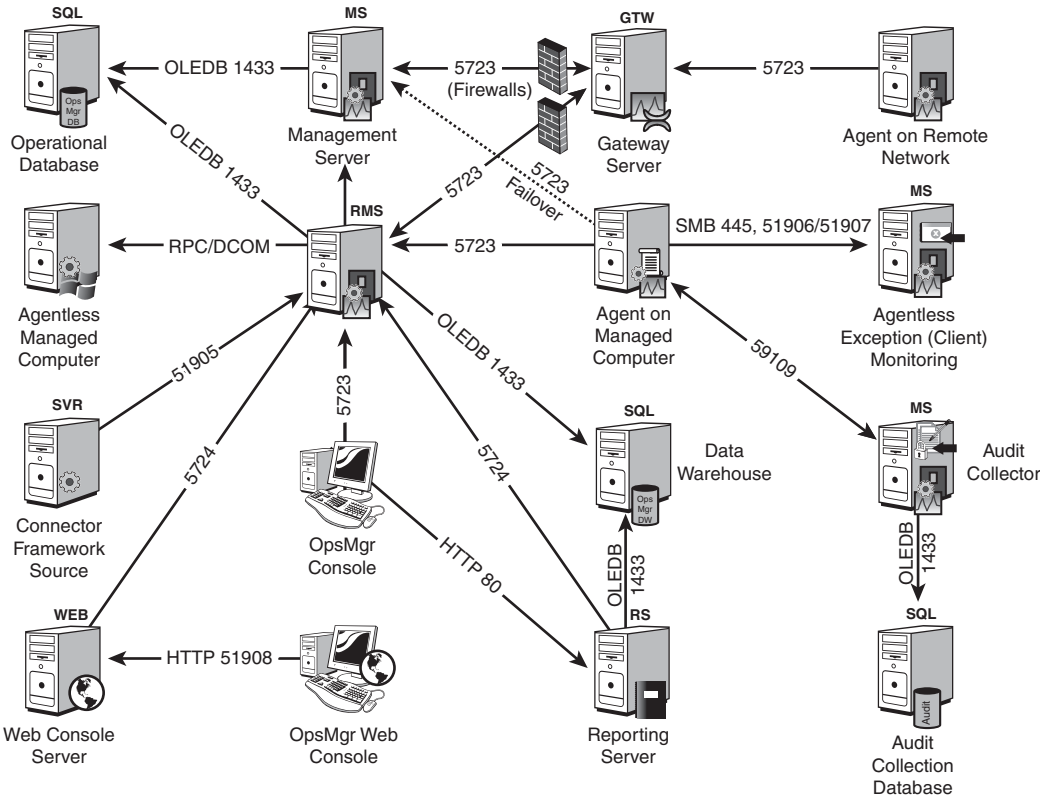


FIGURE 3.5    Communication channels between computers in a management group.

## How Does OpsMgr Do It?

So far in this chapter, we have covered what a management group is, and how the components, or computer roles, of a management group communicate with one another—the macro view. Now we shift our focus to the micro view of the management pack—the computer and device management work the whole OpsMgr infrastructure was deployed for. The management group is the framework within which management packs do that work.

Operations Manager 2007 is a product established on the concept of model-based management. The abstraction of services into *models* is needed to describe and act on physical entities such as routers, and logical entities such as distributed applications, using software

tools that by definition exist in cyberspace. Using models is a way to transform human knowledge and experience into something machines can operate with. In OpsMgr, service models live inside management packs. The management pack author or vendor encapsulates service health knowledge into the redistributable management pack.

Having a solid, accurate model of an object's health lets OpsMgr 2007 present information to the operator in the most immediately useful way. As you will see, the models underpin both the OpsMgr 2007 application, with a workflow framework, and the OpsMgr 2007 operator, with augmented and accelerated decision making.

Operations Manager 2007 introduces an architecture that sets the foundation for a new, broader spectrum of monitoring capabilities and extensibility than has ever been available before using Microsoft management technologies. OpsMgr 2007 fundamental concepts include service and health modeling (we will explain and differentiate between those terms). We'll briefly cover the schema of a management pack so that you understand how a service model is distilled into actionable components such as monitors and tasks. In addition, we will illustrate how monitors are the intersection between the models, and how health information progresses inside the OpsMgr workflow engine to its presentation in the OpsMgr console.

## Service Modeling

One can capture knowledge through models! Service modeling in Operations Manager 2007 is rooted in the well-known Service Modeling Language (SML) used by Microsoft developers in the .NET development environment. SML is an extensible language, built for describing the cooperating systems found not just inside the computer, but also inside an entire datacenter. SML provides a way to think about computer systems, operating systems, application-hosting systems, and application systems—as well as how they interact and are combined, connected, deployed, and managed. SML is used to create models of complex IT services and systems.

A software engineer authoring in Visual Studio Team Edition for Software Architects uses SML to define how an application interacts with various layers of the datacenter, such as the hardware layer, where the servers and routers live, and the operating system layer, which is “hosted” by the hardware layer. The SML concept of one layer hosting another is used in OpsMgr service modeling when relationships are defined between objects managed by OpsMgr, such as a hard drive that hosts a website.

OpsMgr 2007 operates on a class-based structure. When the monitoring infrastructure discovers an “object” (or entity), it assigns a set of logical classes to the object. These classes serve as descriptors for the managed object. The SML for a managed object is imported into OpsMgr using the vehicle of the management pack. Specifically, the management pack adds the formal definitions of “types of objects” (or classes), their properties, and the relationship between objects in the management group. Relationships usually take the form of a dependence on another object, or of a container of another object.



Without management packs and the knowledge they deliver, any OpsMgr group is just a big empty brain. You can compare a management group to the brain, which is a physical structure; in contrast, management packs are analogous to the memories and ideas that live in that brain. Useful thoughts are crafted in the brain based on knowledge and experience. Useful workflow in a management group is made possible by management packs.

We can continue to use a biological metaphor to explain the way management packs convert human knowledge and experience into actionable machine workflows. In the medical profession, a very precise lexicon exists to describe objects in the body. If you think of the parts of your body, you realize the many classes, properties, and relationships that exist. Here are some examples to get you thinking this way:

- ▶ You have a sensory organ “class” that include “objects” such as your eyes, ears, tongue, nose, and skin.
- ▶ Many objects in your body need to be described along with a property or qualifier, such as “left” or “right,” or “proximal” or “distal” to distinguish the particular body part (object).
- ▶ Every object in the body has one or more relationships with other objects, such as the hand “depending” on the arm, or arteries that “contain” blood.

Classes, objects, and relationships are how OpsMgr recognizes an object, understands what the object is, and how to work with the object. Just as we more precisely describe a particular body part by adding the descriptor “left” to the object “hand,” OpsMgr describes objects using a hierarchical system of descriptors that are increasingly specific.

Now you will see this SML layer concept in action as we describe a particular object, a website running on a managed Windows server. See the diagram in Figure 3.6, starting in the upper-left portion of the description, the *Entity*. This is another word for “object” in OpsMgr, and it’s like a placeholder for the object’s root.

Proceeding down and to the right in the hierarchy, or “tree,” depicted in Figure 3.6, we add descriptors to successively narrow, or focus, the description of the particular managed object. As depicted, the Windows Computer Role is a subordinate descriptor to Computer Role. Likewise, the Internet Information Services (IIS) service is a particular Windows Computer Role in OpsMgr, and the monitored website is a particular feature of the IIS service.

Also illustrated in Figure 3.6 are relationships between objects, such as the Windows Operating System (OS) hosting the IIS service, and a particular disk drive hosting the monitored website—which is the object of interest in this description.

The ability of management packs to define relationships between objects, using such terms as “reference,” “using,” “hosting,” and “containing,” is critical to technological innovations found in OpsMgr over previous Microsoft management technologies. OpsMgr features such as monitoring distributed applications with containment relationships, diagrammatic cross-platform fault identification, and maintenance mode on individual computer components are possible via SML and its layered approach to describing objects.

## DESCRIBING OBJECT TYPES IN OPERATIONS MANAGER 2007

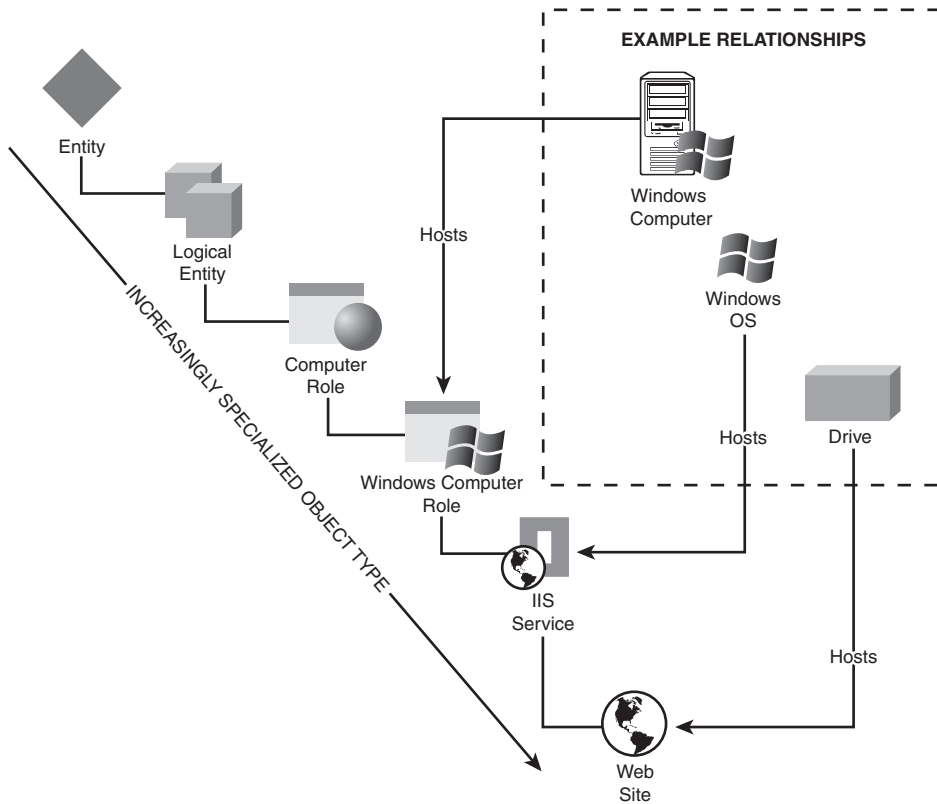


FIGURE 3.6 Describing an object using the System Modeling Language.

Management pack authors include the ability to discern both objects and relationships between objects in the discovery process. Objects and relationships are discovered with probes that examine computer registries using Windows Management Instrumentation (WMI) queries, scripts, database queries (OLE DB), the Lightweight Directory Access Protocol (LDAP), and custom or “managed” code.

We’re going to dive right into an advanced view of the Authoring space to highlight the importance of the process to discover both objects and their relationships in order to understand how OpsMgr works. In Figure 3.7, observe the OpsMgr Authoring space, focused on the Object Discoveries branch of the Management Pack Objects section. In the upper portion of the center pane, notice we have expanded three discovered type classes:

- ▶ Windows Server 2003 Disk Partition
- ▶ Windows Server 2003 Logical Disk
- ▶ Windows Server 2003 Physical Disk

Arrows on the left in Figure 3.7 point to object discovery rules (distributed in the Windows Server 2003 Base OS management pack) that discover disk partitions, logical disks, and physical disk attributes using WMI queries. In the lower (Details) portion of the center pane, we can see the actual WMI query strings used when discovering Windows logical disks (in this case looking for attributes such as what file system is in use and whether the volume is compressed).

Of course, disk partitions as well as logical and physical disks are highly interrelated object classes. Physical disks can contain multiple disk partitions, which in turn may contain multiple logical disks. Logical disks can span multiple disk partitions and physical disks.

Notice in Figure 3.7 that the target column of the discovery rules for a particular object type such as “Windows Server 2003 Disk Partition” identifies the object type that hosts the discovered type. For example, the Windows Server 2003 Operating System (OS) hosts Windows disk partitions; therefore, the Discover Windows Disk Partitions object discovery rule targets the Windows Server 2003 OS object type (or class).

Relationship discovery rules operate in addition to object discovery rules. Object discovery rules use WMI or other probes to locate managed objects and populate the Operations database with actionable object attributes. This enables relationship discovery rules to look at object properties for particular discovered attributes that indicate a dependence, hosting, or containing relationship.

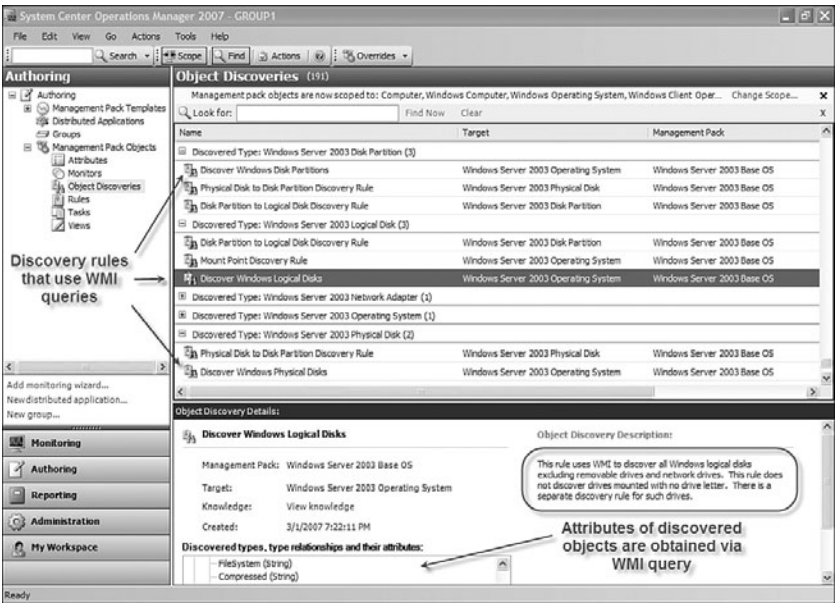


FIGURE 3.7    Probes such as WMI and Registry key queries discover object attributes.

After the Windows Server 2003 Base OS management pack discovers various disk objects, it also discovers the relationships between these classes of disk objects using separate relationship discovery rules. See the relationship discovery rules called out in Figure 3.8. The four relationship discovery rules in this example identify the relationships between physical disks and disk partitions, and between disk partitions and logical disks.

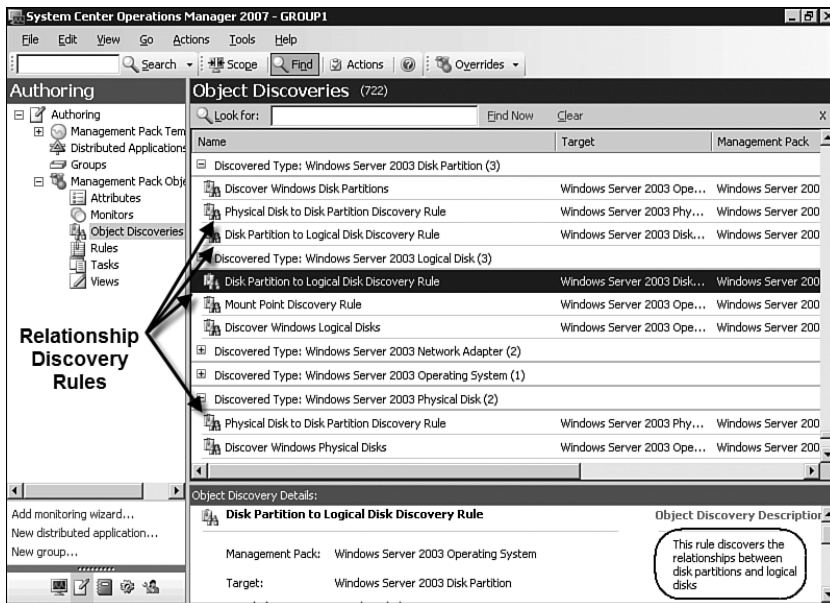


FIGURE 3.8 Both object and relationship discovery rules are associated with most object types, or “classes.”

## Health Models

After object and relationship discovery is complete, the Operations database is populated with the object's descriptive data (its attributes). Now OpsMgr can begin performing the primary work of the management pack, managing the state of the object's health model.

Every class, or object type, has a health model. The status, or health, of even the simplest managed object is represented by a health model. A *model* is a collection of monitors. We will be covering monitors in detail later in the “Monitors” section of this chapter. As we add monitors, we enrich the health model.

Monitors are arranged in a tree structure that is as deep or as shallow as required. The status of the health model represents the current state of the object. The Health Explorer shows a live view of an object's health model. The Health Explorer tool can be launched against any managed object from all views in the Monitoring pane of the console.

A key monitoring concept in OpsMgr 2007 is the *rollup*. We first heard this term from Microsoft early in OpsMgr development, used to describe the way health status “bubbles up” from lower levels in the health model hierarchy, or tree, to higher-level monitors. The top-level monitor in a health model, located at the root Entity object layer, is the rollup, which represents the overall health state of the object.

We return to the Service Modeling Language layer-based method of classifying objects introduced along with the concept of service modeling. Figure 3.9 diagrams (on the left side) the tree-like class hierarchy of the IIS service on a Windows computer. Notice the unit monitors located at the lower right of the diagram inline with the IIS service. Monitors in

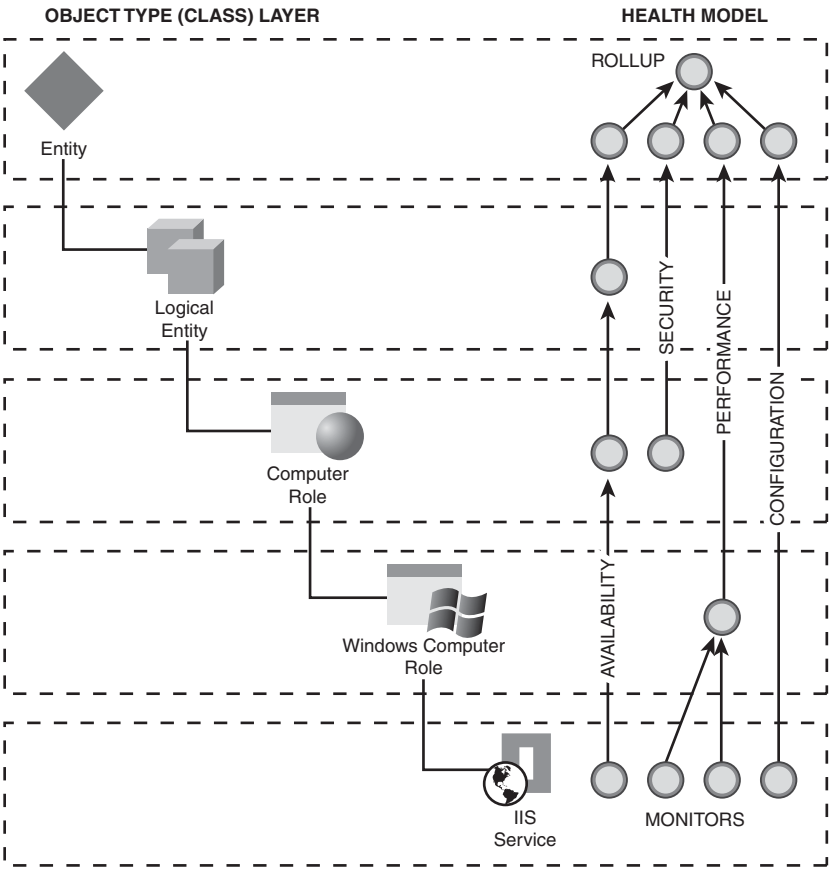


FIGURE 3.9 The layers of SML allow for tactical placement of hierarchical monitors.

each of the four basic categories (Availability, Security, Performance, and Configuration) are represented by round “pearl” shapes.

Lower-layer monitor status is propagated by the health model up to monitors in successively higher layers. For any given health model, monitors are not necessarily located at every layer, or within every monitor category. The management pack author determines what monitors are targeted against what object classes.

Finally, notice in Figure 3.9 the uppermost, triangular arrangement of four monitors rolling up into the health state for the managed object. The rollup occurs at the entity level; this is a universal feature of OpsMgr object health models. The second-level monitors that roll up into the top-level state monitor are called *aggregate monitors*.

## State-based Management

Another key theme in OpsMgr is the employment of *state-based management*, in contrast to previous versions of Operations Manager that were alert-based. An alert-based management system watches for a condition, raises an alert, and optionally changes the state of the object due to the generation of the alert.

The point of the Health Explorer is to illustrate the state of a managed object's health, not to present a list of new or unacknowledged alerts that require operator evaluation. MOM 2005 administrators already know the difficulty in rapidly correlating and triaging a laundry list of alerts in order to answer the question, “What do we need to do to fix the problem?”

The OpsMgr implementation of state-based management applies the following workflow sequence:

1. A unit monitor watches for a condition.
2. When the unit monitor detects the condition, it changes the state of the unit monitor.
3. Unit monitor states are rolled up as required to higher-level aggregate monitors in the object's health model.
4. Rules optionally generate an alert or initiate a notification event.

## Management Pack Schema

A management pack is an eXtensible Markup Language (XML) document that provides the structure to monitor specific software or hardware. A sealed managed pack is a read-only, encrypted version of the XML document. This XML document contains the definitions of the different components in software or hardware and the information needed by an administrator who must operate that application, device, or service efficiently.

We will take a quick look at the schema of the management pack so that you can appreciate how tightly management pack construction is aligned with the health model of an object. A high-level view of the management pack schema is diagrammed in Figure 3.10. From the management pack root, moving right, there are eight major sections: Manifest, TypeDefinitions, Monitoring, Templates, PresentationTypes, Presentation, Reporting, and LanguagePacks.

Only the Manifest section is mandatory, and that section is expanded in the upper-right portion of Figure 3.10. The Manifest section defines the identity and version of the management pack as well as all other management packs it is dependent on. The Identity, Name, and References sections are common and included in every management pack. Any management packs referenced must be sealed, and they must be imported to the OpsMgr management group before the management pack can be imported.

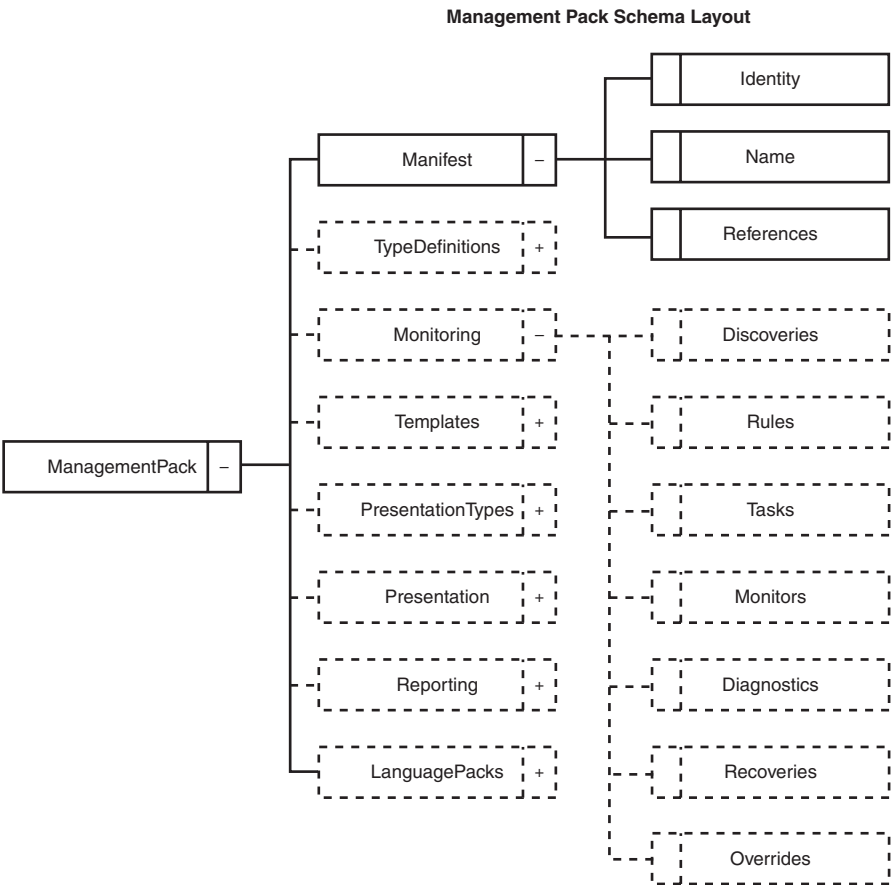


FIGURE 3.10 Management pack schema, with the Manifest and Monitoring sections expanded.

The other major schema section that is expanded in Figure 3.10, Monitoring, is where most of the action takes place in OpsMgr, and this chapter also is mainly about the sections you see contained there. The following list summarizes the purpose of each section of the Monitoring schema:

- ▶ **Discoveries**—A *discovery* is a workflow that discovers one or more objects of a particular type. A discovery can discover objects of multiple types at one time. As introduced previously in the “Service Modeling” section of this chapter, there are both object discovery and relationship discovery rules.
- ▶ **Rules**—A *rule* is a generic workflow that can do many different things. As an example, it could collect a data item, alert on a specific condition, or run a scheduled task at some specified frequency. Rules do not set state at all; they are primarily used to collect data to present in the console or in reports and to generate alerts.
- ▶ **Tasks**—A *task* is a workflow that is executed on demand and is usually initiated by a user of the OpsMgr console. Tasks are not loaded by OpsMgr until required. There are also agent-initiated tasks, where the agent opens up a TCP/IP connection with the server, initiating the communication. After the connection is established, it is a two-way communication channel.
- ▶ **Monitors**—A *monitor* is a state machine and ultimately contributes to the state of some type of object that is being monitored by OpsMgr. There are three monitor types: aggregate (internal rollup), dependency (external rollup), and unit monitors. The unit monitor is the simplest monitor, one that simply detects a condition, changes its state, and propagates that state to parent monitors in the health model that roll up the status as appropriate. We cover monitors in more detail in the next section of this chapter.
- ▶ **Diagnostics**—A *diagnostic* is an on-demand workflow that is attached to a specific monitor. The diagnostic workflow is initiated automatically either when a monitor enters a particular state or upon demand by a user when the monitor is in a particular state. Multiple diagnostics can be attached to a monitor if required. A diagnostic does not change the application state.
- ▶ **Recoveries**—A *recovery* is an on-demand workflow that is attached to a specific monitor or a specific diagnostic. The recovery workflow is initiated automatically when a monitor enters a particular state or when a diagnostic has run, or upon demand by an operator. Multiple recoveries can be attached to a monitor if required. A recovery changes the application state in some way; hopefully it fixes any problems the monitor detected!
- ▶ **Overrides**—Overrides are used to change monitoring behavior in some way. Many types of overrides are available, including overrides of specific monitoring features such as discovery, diagnostics, and recoveries. Normally the OpsMgr administrator or operator sets overrides based on his specific, local environment. However, in some cases, a management pack vendor may recommend creating overrides in particular scenarios as a best practice.



## Monitors

It all starts with monitors in Operations Manager 2007. We have mentioned that a health model is a collection of monitors. If you were to author a management pack, you would probably start with creating unit monitors. Unit monitors would detect conditions you determine are essential to assess some aspect of the health of the application, device, or service needing to be managed.

Monitors provide the basic function of monitoring in OpsMgr. You can think of each monitor as a *state machine*, a self-contained machine that sets the state of a component based on conditional changes. A monitor can be in only one state at any given time, and there are a finite number of operational states.

A monitor can check for a single event or a wide range of events that represent many different problems. The goal of monitor design is to ensure that each unhealthy state of a monitor indicates a well-defined problem that has known diagnostic and recovery steps.

Using a single monitor to cover a large number of separate problems is not recommended, because it provides less value. We mentioned in the lead-in to the “Health Models” section of this chapter that adding monitors to a health model increases the richness of an object’s monitoring experience. The enhancement of an object’s health model with many monitors adds fidelity to the health state of the object. More monitors in a health model also means more relationship connection points for other managed objects that host, contain, depend on, or reference that object.

We pointed out the “pearl” icon used to represent a monitor in health model diagrams. An empty pearl icon represents a generic or a non-operational monitor. Figure 3.11 is a chart showing the default monitor icon images and their corresponding operational state.

A functioning monitor displays exactly one of the primary state icons: green/success, yellow/warning, or red/critical. A newly created or nonfunctional monitor will show the blank pearl icon. The gray maintenance mode “wrench” icon appears in all monitoring views inline with the object that was placed in maintenance mode. The final type of state icon you will encounter is the grayed state icon, which indicates that the managed object is out of contact. For example, this could reference a managed notebook computer that is off the network at the moment.

To be clear, there are three kinds of monitors that management pack authors can create: aggregate rollup monitors, dependency rollup monitors, and unit monitors. In the next sections we will describe each of these monitor types.

### Aggregate Rollup Monitors

Let’s return to the Figure 3.9 view of the layers of the SML, which permits tactical placement of interrelated monitors. On the right, notice the monitors are classified in categories, essentially four vertical columns that are connected by a rollup to the top-level entity health status. Microsoft selected these four categories during OpsMgr development as a framework to aggregate the health of any managed object.

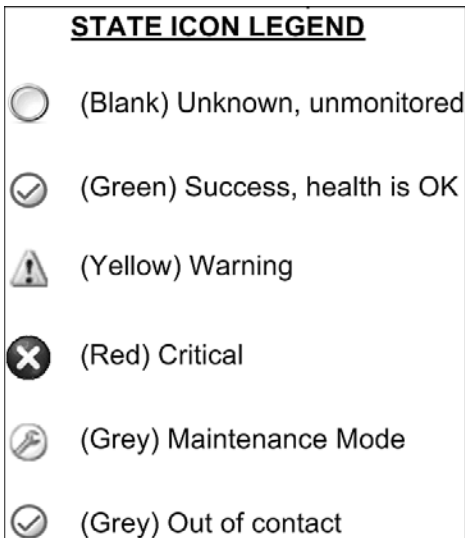


FIGURE 3.11 These state icons are encountered in the Operations console.

The four standard types of aggregate monitors in a state monitor are detailed in the following list:

- ▶ **Availability Health**—Examples include checking that services are running, that modules within the OpsMgr health service are loaded, and basic node up/down tracking.
- ▶ **Performance Health**—Examples include thresholds for available memory, processor utilization, and network response time.
- ▶ **Security Health**—Monitors related to security that are not included in the other aggregate monitors.
- ▶ **Configuration Health**—Examples include confirming the Windows activation state and that IIS logging is enabled and functioning.

### Dependency Rollup Monitors

The second category of monitor is the dependency rollup. Such a monitor rolls up health states from targets linked to one another by either a hosting or a membership relationship. Dependency rollup monitors function similarly to aggregate rollup monitors, but are located at intermediate layers of the SML hierarchy.

In Figure 3.9, notice again the unit monitors for the IIS service located in the lower right. There are two unit monitors of the performance type at the IIS Service level that merge at the Windows Computer Role level. The merge point represents one or more dependency rollup monitor(s) targeted at the Windows Computer Role.

Earlier in the “Service Modeling” section of this chapter, we explored how objects such as disk partitions, logical disks, and physical disks have numerous relationships. Figure 3.12 shows a sample dependency rollup monitor involving disk systems created in the OpsMgr authoring space.

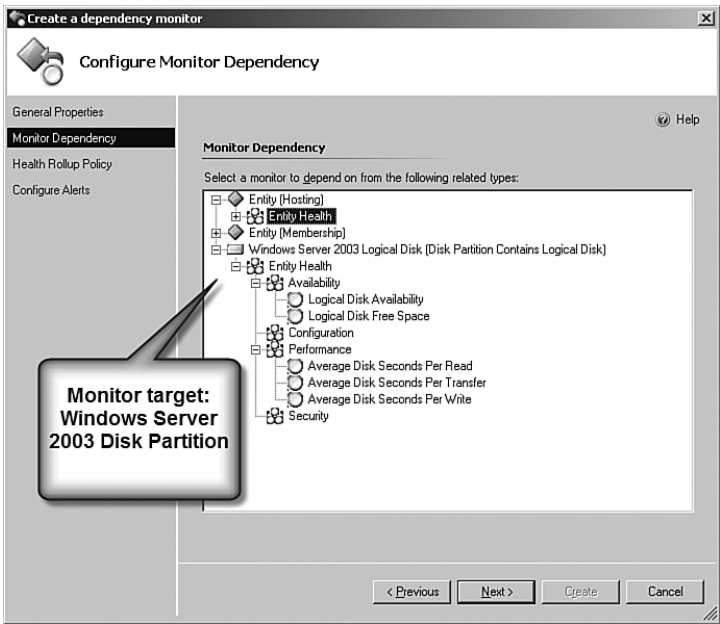


FIGURE 3.12 Creating a dependency rollup monitor when the target is a disk partition.

The monitor created in Figure 3.12 is targeted against the Windows Server 2003 Disk Partition class. OpsMgr knows that disk partitions contain logical disks, so when you create a new dependency rollup monitor targeting the Windows Server 2003 Disk Partition class, OpsMgr offers existing monitors to select from for the Windows Server 2003 Logical Disk class.

We can also expand the example of the “merged” IIS service performance unit monitors in Figure 3.9. If we were creating that dependency rollup monitor in the authoring space, we would have selected the Windows Computer Role as the target of our monitor. The Create a Dependency Monitor Wizard would provide us with a list of dependent objects to select from that includes those IIS service performance monitors.

## Unit Monitors

A unit monitor allows management pack authors to define a list of states and how to detect those states. A simple unit monitor is a Basic Service Monitor. This monitor raises state changes when a Windows service stops running. More complex unit monitors run scripts, examine text logs, and perform Simple Network Management Protocol (SNMP) queries. A unit monitor is deployed, or targeted, at a class of objects when it is authored.

### TIP

#### Target the Agent to Deploy a Monitor to All Computers

Targeting a monitor at the Agent object class deploys the monitor to all managed computers. Use the Agent target like an “All Computers” group for monitors, but also use it sparingly. It is an OpsMgr best practice to deploy the minimum set of appropriate monitors to a managed computer.

When creating monitors and envisioning operational states, Microsoft advises OpsMgr administrators and management pack authors to do so without initially regarding actual implementation of those monitors. The reasoning is that OpsMgr not only provides many monitor types by default for common scenarios, but makes it possible to build different workflows to meet any monitoring requirement. Basically, the management pack architect is encouraged to think “outside the box” and describe in plain ideas how an application’s health can be assessed. After that, you can look to the many tools OpsMgr provides to instrument the application accordingly.

Figure 3.13 presents a montage screenshot that includes all possible types of unit monitors available in the authoring space of the OpsMgr console. These are the tools used to architect the instrumentation of the health model.

Over 50 unit monitor types are available to place as software instrumentation in the SML framework. Remember that unit monitors roll up into the aggregate monitors (Availability, Performance, Security, and Configuration), sometimes via dependency rollup monitors. The goal of monitor design is to ensure that each unhealthy state of a monitor indicates a well-defined problem that has known diagnostic and recovery steps. Table 3.2 provides some explanation of the unit monitor types found in the menu in Figure 3.13.

To conclude this section on monitors, we’re going to put it all together by overlaying the SML and the health model for a live service monitor. Figure 3.14 is a fully expanded view of the health model of the OpsMgr Health service itself running on a management server.

Beginning at the lowest level of the object description tree, we see the MonitoringHost Private Bytes Threshold unit monitor on the computer Hurricane. Five unit monitors are shown in the lowest row that roll up into the Health Service Performance monitor. These unit monitors are labeled with the abbreviations Svc Handle, Svc Priv, Mon Handle, Mon Priv, and Send Queue in Figure 3.14. The MonitoringHost Private Bytes Threshold (abbreviated Mon Priv) unit monitor is in a critical state.

TABLE 3.2    Unit Monitor Types

Monitor type	Description
Average Threshold	Average value over a number of samples.
Consecutive Samples over Threshold	Value that remains over or below a threshold for a consecutive number of minutes.
Delta Threshold	Change in value.
Simple Threshold	Single threshold.
Double Threshold	Two thresholds (monitors whether values are between a given pair of thresholds).
Event Reset	A clearing condition occurs and resets the state automatically.
Manual Reset	Event based; wait for operator to clear.
Timer Reset	Event based; automatically clear after certain time.
Basic Service Monitor	Uses WMI to check the state of the specified Windows service. The monitor will be unhealthy when the service is not running or has not been set to start automatically.
Two State Monitor	Monitor has two states: Healthy and Unhealthy.
Three State Monitor	Monitor has three states: Healthy, Warning, and Unhealthy.

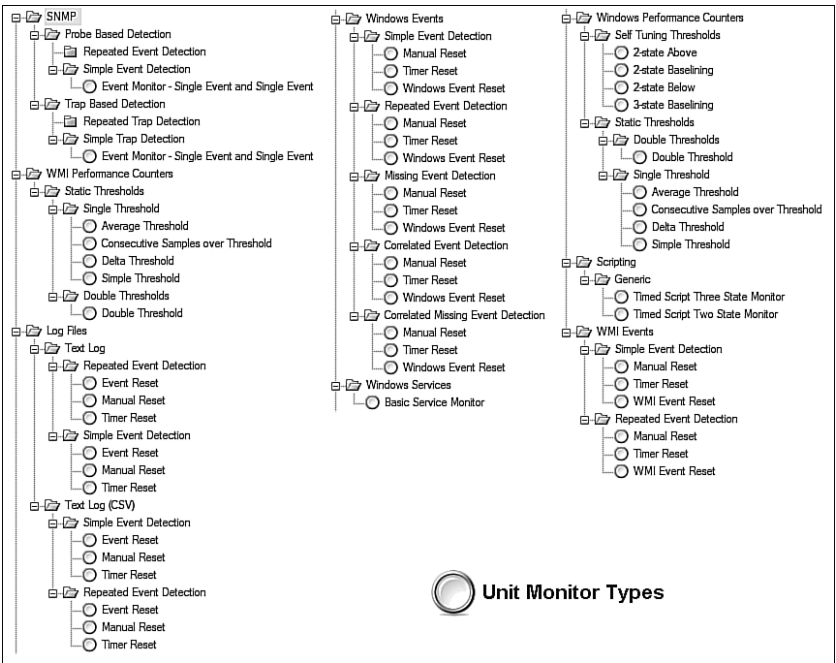


FIGURE 3.13    The complete menu of types of unit monitors that can be created.

We can follow the propagation of this unit monitor state up the health model. The OpsMgr Health service is an application component of Windows Local Application Health Rollup. The Health Service is in a critical state due to the critical state of the MonitoringHost Private Bytes Threshold (abbreviated Mon Priv) unit monitor. Progressing upward, the application state is rolled up along with the hardware, OS, and computer states to the performance component of the object.

The critical state is propagated to the application component of the performance monitor. Finally at the top of the health model, an aggregate monitor rolls up the performance, availability, security, and configuration monitors. The root entity, which is the server Hurricane itself, indicates the aggregated health state, which is critical.

Figure 3.15 shows the Health Explorer for the computer in the state illustrated in Figure 3.14. If you noticed the critical state of the computer in the Monitoring pane of the Operations console, you would probably open the Health Explorer for the computer, which allows you to understand quickly what is wrong. By comparing the structure of the Health Explorer in Figure 3.15 with the SDK and health model layers presented in Figure 3.14, you can match up the same critical health icons in the health model and the Health Explorer.

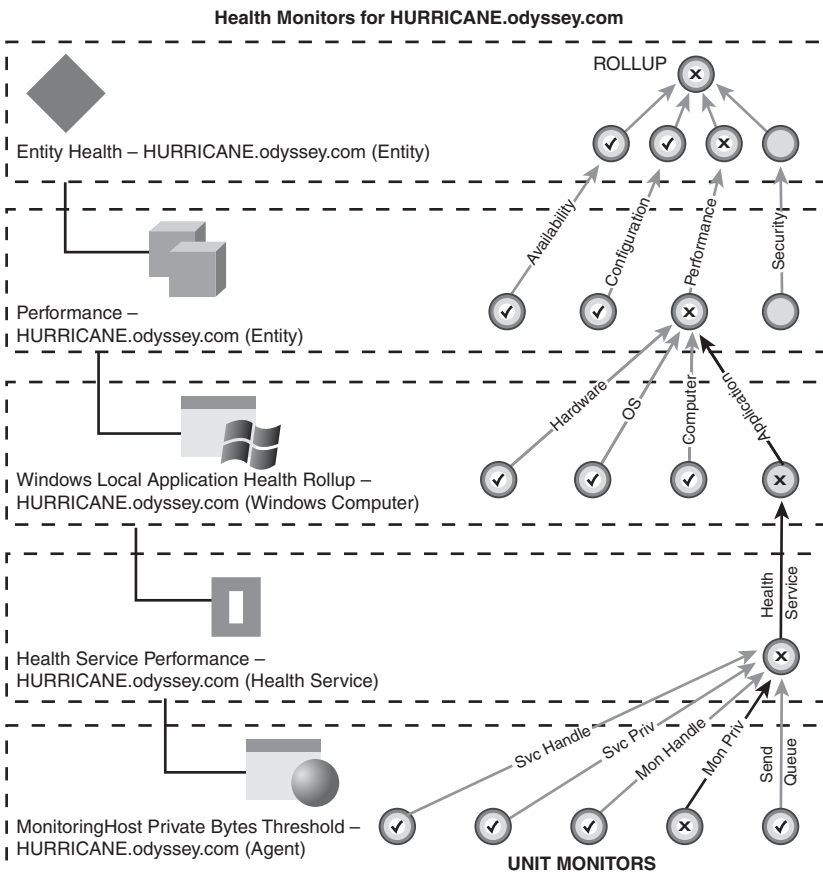


FIGURE 3.14 Expanded view of the health model for the OpsMgr Health Service.

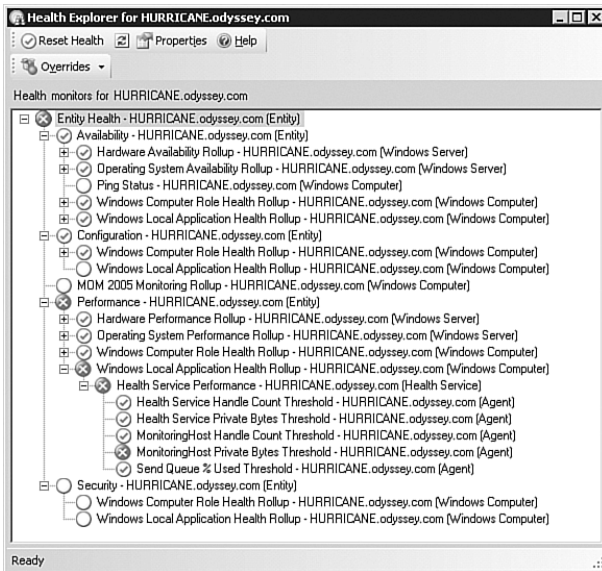


FIGURE 3.15 Health Explorer screenshot of the health model detailed in Figure 3.14.

## Workflow

It is accurate to describe Operations Manager 2007 at its core as being a giant workflow engine. In fact, monitoring in OpsMgr is based around the concept of workflows. An Operations Manager agent and server will run many workflows simultaneously in order to discover and monitor applications, devices, and services.

## Module Types

Module types are the building blocks of Operations Manager workflows. Workflows are defined in management packs and then distributed to managed computers. Workflows can do many things, including collecting information and storing data in the Operations database or data warehouse, running timed scripts, creating alerts, and running on-demand tasks. Workflows are defined using modules, and modules are defined to be of a particular type known as a *module type*. Four different module types can be defined: data source, probe action, condition detection, and write action. Figure 3.16 illustrates these module types.

In the “Architectural Overview” section of this chapter, we compared the management group and management pack to macro and micro views that answer the question “How does OpsMgr do it”? In this section, we are going sub-micro! At the programmatic level, these are the terms and data flow structures used internally by the OpsMgr services:

- **Data Source**—A data source module type generates data using some form of instrumentation or some timed trigger action. As an example, a data source may provide events from a specific Windows event log or it could poll Windows performance counters every 10 minutes for a specific performance counter. A data source takes no

input data and provides one output data stream. Data sources do not change the state of any object.

- ▶ **Probe Action**—A probe action module type uses some input data to provide some output data. A probe action will interrogate a monitored entity in some way, but it should not affect system state in any way. An example would be running a script that queries WMI to get some data. A probe action is often used in conjunction with a data source to run some action on a timed basis. The probe action module type may or may not use the input data item to affect the behavior. In other words, when triggered, a probe action generates output from external sources. Probe actions have one input stream and one output stream. Like data source modules, probe action modules do not change the state of objects.
- ▶ **Condition Detection**—A condition detection module type filters the incoming data in some way. Examples of filter types include a simple filter on the input data, consolidation of like data items, correlation between multiple inputs, and averaging performance data. A condition detection module type can take one or more input data streams and provides a single output data stream. Condition detection modules do not use any external source and do not change object state.
- ▶ **Write Action**—A write action module type takes a single input data stream and uses this in conjunction with some configuration to affect system state in some way. This change could be in the monitored system or in Operations Manager itself. As an example, the action may be to run a script that writes data into the Operations database, or one that generates an alert. A write action may or may not output data. This data cannot be passed to any other module because the write action is the last module in a workflow. However, the data may be sent to the Operations database. A sample action is running a command that outputs data, such as a command line that returns a report of success or errors. This data may be useful to the operator who executes the command, and it is returned to the Operations console and stored as task output.

**Monitoring Workflow Module Types**

Data Source	Probe Action	Condition Detection	Write Action
Does not take input, generates output based on external sources. Does not change object state.	One input and one output; when triggered, generates output from external sources.	One or more input streams, one output. No external sources and no state changes.	One input and zero or one output streams. Changes object state. Always the last module.

FIGURE 3.16 Workflow in OpsMgr is performed through four specific module types.



**TIP****Probe Actions Can Cause Unintended State Changes**

Changes to object states should only occur in response to write action modules. Take note that Operations Manager cannot determine if a probe action is being used to change an object's state in some way. For example, if you run a script that is part of a probe action module type, you could be changing object state in some way in your script. It is up to the management pack author to adhere to the module type definition guidance. If you are changing system state, you should use a write action module type instead.

---

**“Cook Down”**

Cook down is an important concept in management pack authoring. The Operations Manager agent or server is running many hundreds or even thousands of workflows at any given time. Each workflow that is loaded takes some system resource. Obviously the less system resources we take up for monitoring, the better.

The management pack author can do a lot to reduce the impact of monitoring on the system. One way is to ensure that workflows are not targeted too generically. We mentioned this already in this chapter, in the section on “Unit Monitors.” For example, if you have a rule that is only applicable to servers running Microsoft ISA Server 2006, don't target the rule at all Windows servers; instead, you should target it at the appropriate ISA Server class.

Cook down is not about targeting; it is a principle whereby in most modules the Operations Manager Health service will try to minimize the number of instances in memory. This is accomplished by considering the configuration of modules. Usually, if the Health service sees two modules with the same configuration in different workflows that have the same configuration, it will only execute a single module and feed the output to all the workflows that defined the module. This is an efficiency you should be aware of, particularly if you will be authoring scripts for use by OpsMgr.

Here is a simple example of two rules that will “cook down”:

- ▶ **Rule 1**—Collect an event from the application log where Event ID =11724 and Event Source = MsiInstaller (application removal completed).
- ▶ **Rule 2**—Collect an event from the application log where Event ID =1005 and Event Source = MsiInstaller (system requires a restart to complete or continue application configuration).

Operations Manager sees that the event log provider data source (application log events) is configured the same for both rules. Only one instance of the module will run. The two MsiInstaller event ID rules, or expression filters, will take input data from the output of the same module. A large number of expression filters can be handled by one condition detection module. In the case of the event log provider example, there will normally be

only one module executing for each log being monitored (unless you are running the module under different credentials for different workflows).

Cook down becomes particularly important when writing scripts to be run by OpsMgr, especially when there are scripts running against multiple instances of an object type on the same Health service. If you do not think about cook down, you could end up running many scripts when you could actually run a single script by thinking about configuration and targeting.

### Data Types

We have discussed module types and how they are used by OpsMgr internally to achieve workflow. Obviously, OpsMgr must pass data between modules. The format of this data varies depending on the module that output the data. As an example, a data source that reads from the event log will output a different type of data than a module that reads from a text-based log file. Some module types expect a certain type of data. A threshold module type expects performance data and the module type that writes data to the Operations Manager database expects event data. Therefore, it is necessary for Operations Manager to define and use different data types.

Data types are defined in management packs. However, this definition is merely a pointer to a code implementation of the data type. Operations Manager 2007 does not support extension of the data types provided out of the box.

Data types follow an inheritance model in a manner similar to class definitions, introduced in the “Service Modeling” section of this chapter. Whereas the class hierarchy starts with a base class called `System.Entity`, the data type hierarchy starts with a data type called `System.BaseData`. All data types eventually inherit from the base data type. Examples of data types in the `System.BaseData` class include `Microsoft.Windows.RegistryData` (for a probe action module that examines Registry values) and `System.CommandOutput` (for write action modules that return useful command-line output).

When a module type is defined it must, where applicable, specify the input and output data types that it accepts and provides. These must be valid data types defined in the same management pack or a referenced management pack. When a module is used in a workflow, the data types that the module type accepts and provides must be compatible with the other modules in the workflow.

## Presentation Layer

This chapter has dived into progressively more detailed descriptions of how OpsMgr works at the management group, management pack, and workflow levels. Now we will come up for some air and finish with a discussion of the presentation layer in OpsMgr. This is the part of OpsMgr that you see with your eyes and will work with on a continuous and routine basis.

As with any user-level application (as opposed to an application designed only to be run in the background by machines as a Windows service) the presentation layer in OpsMgr is

responsible for delivering and formatting relevant and interesting information to the user or operator. The main interface for Operations Manager 2007 is the Operations console. For doing monitoring work away from the office, Microsoft provides a web-based console with a subset of the full console's functionality, optimized for monitoring functions. Finally, there is the command-line PowerShell for text-based interaction with OpsMgr.

OpsMgr can deliver management information to users with a variety of external notification techniques, such as email and instant messaging. Examples of those notifications and how they are configured are discussed in detail in Chapter 8, "Configuring and Using Operations Manager 2007." However, OpsMgr cannot be administered and run only through notifications.

**Operations Console**

Unless you are using the Web console from a remote location, or running PowerShell for specialized work, all interaction between operations personnel and the Operations Manager 2007 application will occur using the Operations console. The console is not a Microsoft Management Console (MMC) snap-in, but a standalone application installed on management servers and optionally installed on any supported Windows computer.

The Operations console is composed of several panes, as shown in Figure 3.17, each of which serves a particular purpose. We will be covering the OpsMgr features accessed in the various console panes in detail in Chapter 8.

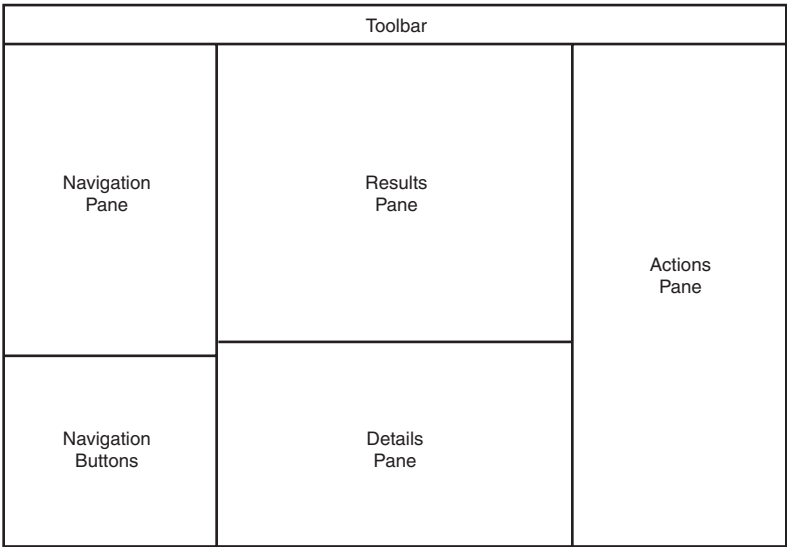


FIGURE 3.17    Layout of the Operations console.

As you can see in Figure 3.17, the OpsMgr console shares some features with the popular Microsoft Office Outlook application, such as the Navigation pane and navigation buttons. The Actions pane shares the look of another contemporary Microsoft application, Exchange 2007 (which also features PowerShell as an integrated component). The navigation buttons in the lower-left corner are a key feature of the console. They provide a rapid, intuitive way to shift between management tasks without firing up other consoles or applications. Here is a quick rundown on those navigation buttons:

- ▶ **Monitoring Pane**—Displays several different types of views that enable operators to analyze monitoring results within the managed environment(s). This is where most users of OpsMgr will spend their time because the Monitoring pane is where the action is!

Views of alerts, events, object states, performance, diagrams, tasks, and dashboards exist here. When reporting is installed, the lower portion of the Actions pane provides context-aware reports for the objects in the Results pane.

- ▶ **Authoring Pane**—Enables creation of additional monitoring objects to customize or supplement the default monitoring settings provided in management packs. New customized management packs can be created using several templates provided with OpsMgr. Custom groups used to target rules are created here. Only administrators and advanced operators have access to this pane.
- ▶ **Reporting Pane**—If OpsMgr reporting is installed in the management group, this pane displays a report library with the reports included in management packs, and it enables editing of customized reports. Only administrators and report operators have access to this pane. This navigation button is not present if reporting is not installed.

The report library contains generic reports, such as Alert Logging Latency and Most Common Events reports. Reports launched from the Reporting pane have no prespecified context, and operators must manually specify the context for the report in the parameter header before running the report. Reporting is discussed in more detail in Chapter 8.

- ▶ **Administration Pane**—Enables editing of high-level Operations Manager settings that affect the entire management group. It also enables viewing and configuring individual management servers and managed objects. The critical Security roles, Run As Accounts, and Run As Profiles are managed here. All work related to adding and deleting agent-managed computers, agentless managed computers, and network devices is performed in this pane. Only administrators have access to this pane.
- ▶ **My Workspace Pane**—Enables creation and storage of console customizations for later reuse. Although OpsMgr administrators can modify the main views and add new views using the Administration pane, there are many occasions where the operator has her own ideas or requirements for monitoring. The My Workspace pane is a personal area where console users can make new customized views to their heart's content and not impact other system users. Users can also store possibly complex search criteria here, saving lots of time on each future occasion when those searches are used.

**TIP****Turn the Navigation Button Area into a Toolbar**

The navigation button area of the Operations console provides a quick way to change the functionality of the Results, Details, and Action panes in the console. However, the default navigation buttons encroach on the more useful Navigation pane above them and occupy almost 10% of the console area. You can recover that space by dragging the grouping bar above the top navigation button downward. This collapses the larger navigation buttons into much smaller icons that resemble a standard toolbar.

---

The center portion of the console, where the Results and Details panes are located, is particularly reconfigurable and divides into as many as nine separate panes in some console views. The Operations console also uses multiple windows, which open like pop-ups, and can be closed without affecting the main console. For example, when Operations Manager features such as override, search, Health Explorer, and Security are being used, new windows open to support the selected operation.

The Find, Search, and Scope buttons in the Operations console make it easier for users to manage data. The Scope and Search controls are located at the top of the console in the toolbar area, and the Find filter is found at the top of the Results pane. Because OpsMgr can manage many thousands of objects, these filtering functions are a critical usability feature in large environments.

## Web Console

Borrowing again from the success of the Outlook interface, which is a very well received, almost identical web interface to Outlook Web Access, Microsoft delivered a Web console for OpsMgr. The Operations Manager 2007 Web console is really a triumph of web interface design and execution. It mimics many features of the Monitoring and My Workspace portions of the full Operations console.

An ActiveX control is downloaded to the user's web browser on his first visit to the Web console from any given computer. If the Web console is installed on a management server, additional notification and access features become available to the management group. Specifically, there is a mobile access feature for smart phones and Personal Digital Assistants (PDAs) with network or Internet access, along with a Really Simple Syndication (RSS) version 2.0 feature that allows operators to set up RSS subscriptions to OpsMgr alerts.

## PowerShell

PowerShell provides a means to interact with the OpsMgr application without any graphical interface. Much of the work that can be done in the Operations and Web consoles can also be done using PowerShell. PowerShell is particularly useful in a variety of specialized situations. Compared to the immensely usable OpsMgr console, it is an adjustment to work with the command line of PowerShell, particularly at first. However, just having the

opportunity to view and set data in the Operations database programmatically using the command line is a fantastic addition to the administrator's toolkit.

We will close this section with an example of the functionality and presentation of PowerShell compared to the OpsMgr console. We created a custom user role in the Security -> User Roles node of the OpsMgr Administration pane, named Partner Staff Acme. In Figure 3.18, you can see the properties of that user role, in a window launched from the console.

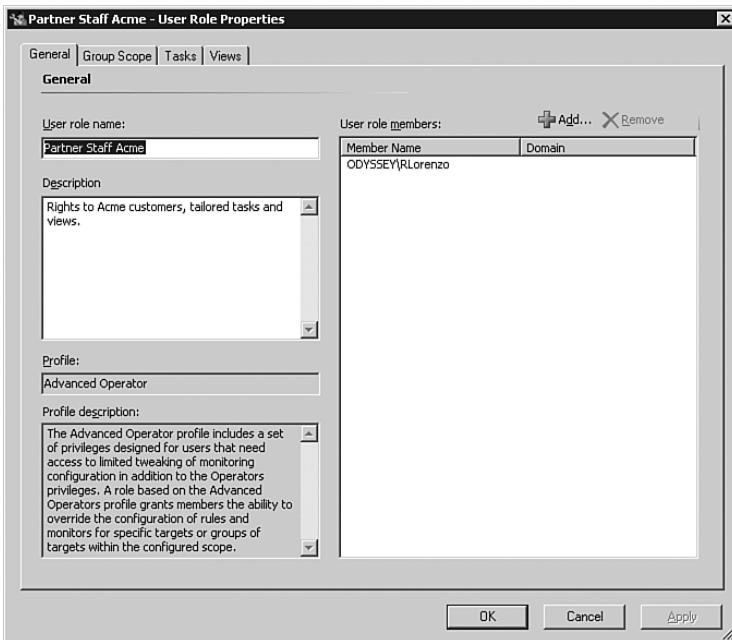
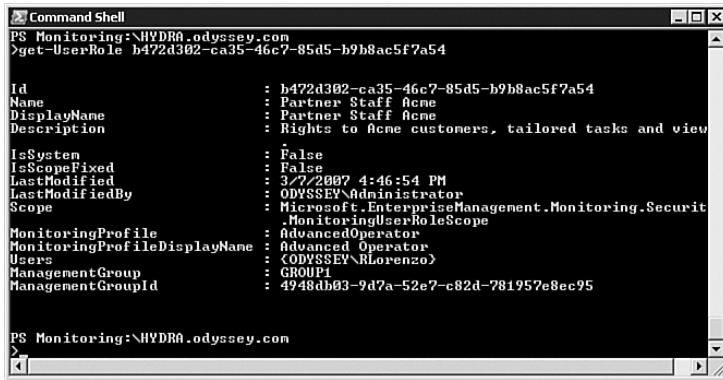


FIGURE 3.18 Properties of a custom user role, viewed with the OpsMgr console.

To access the Properties window in Figure 3.18, you simply right-click the user role in the OpsMgr console and select Properties. Notice that there is one user, Rlorenzo, who is a member of that role in the ODYSSEY domain. Now we will use PowerShell to access the same information.

In Figure 3.19, notice the command window with the output of the PowerShell cmdlet `get-UserRole`. You can see the same information, such as the description of the role and the membership for Rlorenzo. However, to achieve that output, you have to know the GUID (Globally Unique Identifier), a code name that is a long set of alphanumeric characters associated with the Partner Staff Acme user role. To learn the GUID of that role, you first have to use PowerShell to list the GUIDs for all the created and installed user roles. Of course, you also have to learn the syntax of the cmdlet. So there is a learning curve, and a rather brutal interface involved. For the true scripter, however, PowerShell could become

the presentation layer of choice in some situations, and it adds the ability to perform OpsMgr actions in batch mode.



```

Command Shell
PS Monitoring:\HYDRA.odyssey.com
>get-UserRole h472d302-ca35-46c7-85d5-b9b8ac5f7a54

Id                : h472d302-ca35-46c7-85d5-b9b8ac5f7a54
Name              : Partner Staff Acme
DisplayName        : Partner Staff Acme
Description        : Rights to Acme customers, tailored tasks and view
IsSystem          : False
IsScopeFixed       : False
LastModified       : 3/7/2007 4:46:54 PM
LastModifiedBy     : ODYSSEY\Administrator
Scope              : Microsoft.EnterpriseManagement.Monitoring.Security
MonitoringProfile  : MonitoringUserRoleScope
MonitoringProfileDisplayName : Advanced Operator
Users              : <ODYSSEY\RLorenzo>
ManagementGroup    : GROUP1
ManagementGroupId  : 4948db03-9d7a-52e7-c82d-781957e8ec95

PS Monitoring:\HYDRA.odyssey.com
>

```

FIGURE 3.19 Properties of the custom user role shown in Figure 3.18, now viewed with PowerShell.

## Summary

This chapter promised a look inside OpsMgr from the macro and micro perspectives. We described first how OpsMgr components are deployed on a single server to a small organization, or across many servers for the large enterprise. We also closely examined the communication channels used between components. We next covered how management packs encapsulate and distribute knowledge about objects and classes of objects, including relationships between objects. Then we looked even deeper at the workflows occurring between modules in a management pack. Finally, we discussed how the Operations console, Web console, and PowerShell present useful management information to the operator and administrator.

With this information, you are ready for the next two chapters, where we discuss designing an OpsMgr 2007 implementation.

# Symbols

**& (ampersand), in scripts, 663**

**2-state Above baseline, 674**

**2-state Baseline monitor, 674**

**2-state Below baseline, 675**

**3-state Baseline monitor, 675**

## A

### access

ACS reports, 764

with Operations console, 767-769

with SQL Report Manager, 769-770

Exchange accounts, 934

monitoring, 480

multiple domains, 218

**Access Control Lists (ACLs), 390**

**access violation scenario (audit reports),  
786-789**

**account management scenario (audit reports),  
784-786**

### accounts

Action, 492

low-privileged accounts, 493-494

Management Server Action account, 493

modifying credentials, 496

MonitoringHost.exe process, 492

unlocking, 526

Windows 2000/XP, 495

Agent Installation, 499

Computer Discovery, 499

Config Service, 496-499

Data Reader, 500

Data Warehouse Write Action, 499

domains, updating, 495

Exchange access, 934

Gateway Action, 501-502

Health Service, 501

Local Service, 495

Notification Action, 499

requirements, 490-491

Run As Accounts, 488-490

SDK, 253, 496-499

security, 239

**Accvio.exe, 810, 814**

**ACLs (Access Control Lists), 390**

**ACS (Audit Collection Services), 44, 86,  
206-208, 740**

administration of, 766

ACS collector performance, 773-777

with AdtAdmin.exe utility, 770-773

certificate-based ACS forwarders, 782

database size management, 778-780

failover, enabling, 780-782

with Operations console, 767-769

with SQL Report Manager, 769-770

connections to SQL Server named  
instances, 751

dedicated ACS management group, 143

deployment, steps in, 740-741

drivers, permitting, 395

enabling with PowerShell, 763

explained, 108

forwarding, 229

installation, 262-266

network bandwidth utilization, 145

online information, 1305-1306

operating system requirements, 158

planning audit policies, 741-746

planning component deployment, 747-752

ACS collectors, number of, 750-751

clustering ACS database servers, 748

reporting services integration, 749

security boundary, creating, 748-749

SQL Server 2005 Standard versus  
Enterprise editions, 751

security, 526-527, 765

enabling certificate support, 528

encryption, 529

installing certificates, 527-528

SQL Server 2005 editions and, 86

**ACS auditors security group, creating, 753-754**

**ACS clusters, installing, 451-452**



**ACS Collector Component, 227-228, 740**

- clustering, 451-452
- configuring, 752-755
- hardware requirements, 155
- installing certificates, 528
- number of collectors, 750-751
- performance management, 773-777, 1269-1270
- redundancy, 452

**ACS Database Server Component, 227**

- backing up, 541
- clustering, 451
- configuring, 752-755
- data retention period, 765
- granting permissions on, 754-755
- grooming, 553
- hardware requirements, 155
- moving, 569-570
- Registry keys, 1284-1286
- security settings, 756
- size management, 778-780
- system-level management, 765

**ACS Forwarder, 740**

- certificate-based forwarders, enabling, 782
- detailed logging, enabling, 776
- enabling, 760-762
- failover, enabling, 780-782
- hardware requirements, 155
- Registry keys, 1286-1287

**ACS reports. See also audit reports**

- accessing, 764
  - with Operations console, 767-769
  - with SQL Report Manager, 769-770
- backing up, 584
- installing, 756-757
- integration scenarios, 758-760

**Act as Proxy setting, 414****Action account, 492**

- credentials, modifying, 496
- low-privileged accounts, 493-494
- Management Server Action account, 493
- MonitoringHost.exe process, 492
- unlocking, 526

Windows 2000/XP, 495

Windows Server 2003/Vista, 495

**Active Alerts view, 315-317****Active Directory**

- agents, integration, 386-391
- integration, 79-80, 473, 1033-1034
  - planning, 218-219
  - sample script, 730-731
- PowerShell commands for, 1027
- preparing operations manager for ROM, 1065-1067
- sites, creating computer groups based on, 1017
- viewing health with monitors, 959-961

**Active Directory Helper Object (OOMADS), 285****Active Directory management pack (ADMP), 285, 386, 1229**

- AD\_Client\_Connectivity script parameters, 1299
- AD\_Client\_GC\_Availability script parameters, 1300
- AD\_Client\_PDC\_Response script parameters, 1300
- AD\_Database\_and\_Log script parameters, 1296-1297
- AD\_Essential\_Services\_Running script parameters, 1299
- AD\_General\_Response script parameters, 1297
- AD\_Global\_Catalog\_Search\_Response script parameters, 1297
- AD\_Op\_Master\_Response script parameters, 1298-1299
- AD\_Replication\_Monitoring script parameters, 1295-1296
- installation, 1229-1230
- tuning, 724-725, 1230-1235

**Active Directory Topology Root, 954**

- distributed applications, 958-959
  - Diagram view, 962
  - in-line tasks, 961
- viewing health with monitors, 959-960

**adapting to environment, 1008, 1035**

- Active Directory integration, 1033-1034
- Capacity Planner integration, 1024-1025

- computer groups, 1017-1018
- Configuration Manager integration, 1022-1024
- console tasks, 1018-1021
- custom management packs, 1034
- diagnostic tasks, 1008-1012
- distributed applications, 1038-1040
- Exchange 2007 integration, 1031-1033
- notifications, 1015-1016
- PowerShell integration, 1026-1029
- recovery tasks, 1008-1010, 1013-1014
- security adaptations, 1041-1042
- servers, provisioning, 1042-1045
- Service Manager integration, 1029
- SharePoint integration, 1029-1031
- system maintenance, 1035-1038
- user accounts, provisioning, 1040-1041
- Virtual Machine Manager integration, 1025-1026
- VMWare integration, 1034
- Add Monitoring wizard, 910**
- AddReportingUserRole.ps1, 482**
- administration, 471**
  - ACS, 766
    - ACS collector performance, 773-777
    - with AdtAdmin.exe utility, 770-773
    - certificate-based ACS forwarders, 782
    - database size management, 778-780
    - failover, enabling, 780-782
    - with Operations console, 767-769
    - with SQL Report Manager, 769-770
  - security, 471
- Administration Overview page (Operations console), 306**
- Administration pane (Operations console), 131, 357-362**
- administrative control for management groups, separating, 142**
- administrative model in assessment document, 140**
- Administrator role, 78, 483-485**
- ADMP. See Active Directory management pack**
- AdtAdmin.exe utility, 770-773**
- advanced monitoring for websites, configuring, 912-919**
- Advanced Operator role, 78**
- AD\_Client\_Connectivity script parameters, 1299**
- AD\_Client\_GC\_Availability script parameters, 1300**
- AD\_Client\_PDC\_Response script parameters, 1300**
- AD\_Database\_and\_Log script parameters, 1296-1297**
- AD\_Essential\_Services\_Running script parameters, 1299**
- AD\_General\_Response script parameters, 1297**
- AD\_Global\_Catalog\_Search\_Response script parameters, 1297**
- AD\_Op\_Master\_Response script parameters, 1298-1299**
- AD\_Replication\_Monitoring script parameters, 1296**
- AeDebug, applying, 811**
- AEM (Agentless Exception Monitoring), 72, 211, 228, 418, 797, 804**
  - bucket types, 822
  - Configuration Manager integration, 1024
  - clusters, installing, 454
  - implementing, 805-819
  - installation, 268-271
  - licensing, 161-162
  - Resource Kits, 843
  - SLAs, tracking, 819
- Agent Action account, 165**
- Agent Component, 101**
- agent deployment, design stage (deployment planning), 165**
- Agent Health service, 106**
- Agent Installation account, 165, 499**
- Agent objects, targeting monitors at, 123**
- agent proxying, configuring, 358**
- agent tasks, 71, 356, 1018**
- agent-managed computers**
  - clients, monitoring, 828-842
  - in Device Management node, 357
- Agentless Exception Monitoring. See AEM**

**agentless managed systems**

- deleting, 1309
- in Device Management node, 357
- Registry settings, 1274

**agentless monitoring, deployment, 404-405****agents, 83**

- Action account, 492
  - low-privileged accounts, 493-494
  - Management Server Action account, 493
  - modifying credentials, 496
  - MonitoringHost.exe process, 492
  - Windows 2000/XP, 495
  - Windows Server 2003/Vista, 495

AEM. *See* AEM

agentless managed state, 380-382, 404-408

approval process, modifying, 373-374

bandwidth utilization, 179

deployment, 385-386

- Active Directory integration, 386-391
- ConfigMgr, 393-394
- Discovery Wizard, 395-400
- Group Policy, 391-392
- imaging, 395
- manual installation, 402-403
- PowerShell installation, 403-404
- SMS, 393-394

discovery process, 370-373

distributing to management groups, 431

failover servers for, 426-427

firewalls, 532-533

Gateway Server Component, 208

hardware requirements, 156

heartbeat settings, 358-359

installation, 294

maintenance, 195

management, 208, 410, 640

- configuring settings, 414
- defining failover, 414-416
- deleting, 417-418
- disk performance, 412
- event logs, 410-412
- pending actions, 412-413
- queue files, 416-417

migration on same hardware, 281

multihomed agents, 99, 432

mutual authentication, 503-507, 511

network bandwidth utilization, 145

network devices, 384

operating system requirements, 158-159

Operations Manager, 229

performance counters, 1261-1264

proxying, 405-408, 511-512

queue files, 416-417

Registry keys, 1274-1276

remote agents, prerequisites, 385

reporting, 409-410

role of, 39

security settings, 359

SNMP, 846

state management, 374, 378, 380

troubleshooting, 418-422

unknown state, 384

**aggregate monitors, 117, 119-121, 604**

**aggregate rollup monitors, 120, 682**

**aggregated client monitoring, 804, 829**

**aggregation level (datasets), 548**

**AKM file format, 1163**

**AKM2XML resource kit utility, 1163**

**alert latency, 153**

**alert overload, 190**

**alert rules, creating trap-based alert rules (SNMP), 880-887**

**alert text, screen capturing, 698**

**alert-based management, 117**

**alert-generating rules, 603, 649-653**

**alerts, 648, 687-688, 1164**

Active Alerts view, 315-317

Active Directory management pack, 1230-1235

aggregated, 804

closing, 317, 653

context menu tasks, enabling, 1292

creating for monitors, 684-686

debugging, 1309

Dell management pack, 1259-1260

during management pack implementation, 623

- embedding tasks in, 688
- Exchange 2003 management pack, 1237-1249
- forwarding by email, 690
- generating, 688-690
- IIS management pack, 1255
- knowledge, adding, 699-703
- notification workflow, 691-699
- reports, 627-630
- resolution states, 358, 716-718
- resolving, 317-319
- SQL Server management pack, 1251-1253
- state monitors versus, 719
- transitory alerts, 315
- tuning, 718, 723
  - Active Directory management pack, 724-725
  - by color, 718-719
  - Exchange Server 2003 management pack, 723-724
  - SQL Server management pack, 726-727
  - Windows Server Operating System management pack, 726
- viewing, 41-43
  - creating views, 720-723
  - product knowledge, 49-50
- Alerts view (Operations Manager Management Group), 955-956**
- All Events for Specified Computer report, 784**
- All Events for Specified User report, 784**
- All Events with Specified Event ID report, 784, 790**
- ampersand (&), in scripts, 663**
- antivirus software, 1037**
- API (Application Programming Interface), 472**
- appending backups, 556**
- Application Error Group view, 813**
- Application Log Library, 374**
- Application Programming Interface (API), 472**
- Application Service Providers (ASPs), 966**
- Application view, 813**
- applications**
  - design stage (deployment planning), 164
  - distributed applications, 1038-1040
  - errors, events, 812
  - LOB, monitoring, 928-933
  - monitoring, 940-941, 944, 947
  - Top Applications report, 820
  - watcher nodes, 906-907
  - Web, monitoring, 907-909, 912-920
  - Web Application Editor, 912
- applying**
  - AeDebug, 811
  - enterprise CA, 513-515
  - standalone CA, 515-517
- approving**
  - agents, modifying, 373-374
  - customer sites (customer networks), 1085-1087
  - gateway servers, 435-436
- architecture**
  - AEM, 805-808
  - management group design, 146-148
  - online information, 1307
  - of OpsMgr 2007, 98
    - management groups, 98-100
    - server components, 100-105
  - of SNMP, 846-848
- archiving audit reports, 764**
- ASP.NET, installation, 249**
- ASPs (Application Service Providers), 966**
- assessment documents, 141**
- assessment stage (deployment planning), 139-141, 425**
- assignments, roles, 474**
- attributes, 354-355, 639**
- audible alerts, creating, 1016**
- Audit Collection Services. See ACS**
- Audit Collector Component, 103**
- Audit Database Server Component, 103**
- Audit Failures report, 795**
- Audit Forwarding service, 79, 107**
- Audit Log Cleared report, 795**
- audit policies, 740**
  - categories, 744-746
  - implementation, 763-766
  - need for, 739-740

planning, 741-746

Security Event log, 739

**audit reports, 749. See also ACS reports**

access to, 764

access violation scenario, 786-789

account management scenario, 784-786

archiving, 764

consumers of, 764

Forensic category, 784

Planning category, 783

policy changes scenario, 789-794

scheduling, 768-769

system integrity scenario, 794-795

**authentication**

configuring, 919

gateway servers, 432, 434

Kerberos, 217

mutual, 217, 503-507, 511

selection, 253

trusted authentication, running Operations console without, 340-342

**Author role, 78**

**Author user role, creating, 478**

**Authoring pane (Operations console), 75, 131, 352-357**

classes, 1178-1181

overview, 1175-1177

unit monitors, 1182

**authoring security, 471**

**Authorization Manager, 472**

**automatic checkpoints, transaction logs, 561**

**automatically run diagnostic tasks, 1008**

**availability**

configuration planning, 221-229

of Operations database, 108

of RMS, 108

**availability health monitors, 121**

**Availability Monitor (Exchange Services), 967-970**

**Average Threshold monitor, 669**

**AzMan (Authorization Manager), 472**

## B

**BackOffThreshold value (ACS collector performance), 774**

**backups, 576, 586**

of ACS reports, 584

appending, 556

batch file for, 585-586

of data warehouse, 550-553

disk backups, 1037

importance of, 539-540

of management packs

with Operations console, 580-582

with PowerShell scripts, 577-580

naming, 556

of Operations database, 554

importance of, 464

steps in, 554-560

truncating transaction log, 560-563

of OpsMgr reports, 583

overwriting, 556

of RMS encryption keys, 255, 570-572

scheduling, 542-544, 558-560

of SQL Server databases, 553-554

steps in, 554-560

truncating transaction log, 560-563

of SRS encryption keys, 584-585

transaction logs, effect of, 561

of virtual machines, 1037

what to include, 540-542

**bandwidth utilization, 145**

agents, 179

multiple-server configuration example, 175

**Baseline Security Analyzer management pack, 1036**

**baselines, 673-675, 1246-1249**

**Baselining Tasks Library, 374**

**Basic level (IO Model), 33**

**batch files**

for backups, 580, 585-586

launching with timed commands, 663-665

**batch imports of management packs, 329**

**behavior, predicting by simulation, 905**

- Blank templates, 998-1002
- blogs, list of, 1314-1316
- branding for OpsMgr 2007, 67-68
- browsers, 1166
- buckets
  - errors, customizing, 816-818
  - types, AEM, 822
- built-in templates, importing into Local Security Policy, 743
- bulk deployment, 194
- bulk\_logged recovery, 554
- business critical monitoring, 804, 829, 838-843
- business logic tier (distributed applications), 950
- business requirements
  - in assessment documents, 140
  - for design stage (deployment planning), 141

## C

- CA (certificate authority), 512, 1056
  - configuring, 517-519
  - enterprise, 513-515, 1067-1069
  - standalone, 515-517, 1067-1069
  - troubleshooting, 519-520, 523
- .CAB files, 811
- capacity changes in OpsMgr 2007, 91-92
- capacity limitations, design stage (deployment planning), 178-189
- Capacity Planner, 59, 1024-1025
- capture sessions, starting, 914
- capturing Syslog messages, 1135-1137
- case studies, migration, 288-298
- categories
  - of audit policies, 744-746
  - subscriptions and, troubleshooting, 692
- CD, list of files on, 1323
- CEIP (Customer Experience Improvement Program), 359, 798, 823-828
- centralized monitoring system, OpsMgr 2007 as, 37-39
- CER (Corporate Error Reporting), 799-800
- certificate authentication, 432
- certificate authority, 512, 1056, 1067-1070
- Certificate Services, online information, 1306
- certificate-based ACS forwarders, enabling, 782
- certificates
  - OWA certificates, piggybacking, 1082
  - Registry keys, 1293
  - ROM, 1055-1056
  - sealing management packs, 614-615
  - Service Provider Mode (System Center Essentials), 1079
- Changing quadrant (MOF), 30
- Citrix Presentation Server Management Pack, 1118-1119
- class types, 606
- classes, 51
  - creating with Authoring console, 1178-1181
  - objects and, 601
- Client Access role (Exchange 2007), 1031
- Client Business Critical Operating System management pack, 331
- Client Data Source Access feature, 980
  - creating OLE DB Data Sources, 980-981
  - creating Windows Explorer Data Source Service DA, 982-984
  - customizing Data Source Service DA, 984-986
- Client Monitoring Internal Library, 374
- Client Monitoring Library, 374
- Client Monitoring Server Component, 104
- Client Monitoring Views Library, 374
- client OML, 159
- clients
  - Collective Client Monitoring, 832-837
    - management packs, 798
    - monitoring, 85, 211
  - Active Directory Topology Root, 958
  - AEM, 805-819
  - agent-managed systems, 828-842
  - CEIP and Microsoft Privacy Statements, 823-828
  - CER, 799-800
  - cost of end-user problems, 802-803
  - features, 797-798
  - machines, 800-801
  - new features, 803-805

- online information, 1306
  - reporting, 819-823
  - synthetic transaction monitoring, 843
  - Windows Error Reporting, 798-799
- operating systems, monitoring, 379
- closing alerts, 317, 653**
- cluster resource groups, 441**
- clustered RMS, restoring, 576-577**
- clustering**
  - ACS database servers, 748
  - nodes, monitoring, 223
- clusters, 440-441**
  - ACS clusters, installing, 451-452
  - AEM clusters, installing, 454
  - complex database clusters, installing, 452-454
  - data warehouse clusters, installing, 449-451
  - installing, 441-442
  - Operations database clusters, installing, 447-448
  - reporting server clusters, installing, 455-457
  - RMS clusters, installing, 457-467
  - SQL Server 2005 clusters, installing, 443-447
  - testing failover, 442-443
  - validating, 441
  - virtual server clusters, 443
- cmdlets (PowerShell), help information, 1028**
- coexisting agents with MOM 2005, 409**
- collection rules, 603, 653-662**
  - event-based collection rules (SNMP), creating, 888-891
  - performance collection rules
    - creating, 654-656
    - optimized collections, 655-657
  - performance-based collection rules (SNMP), creating, 890-894
  - probe-based rules, 657
  - script rules, 657-662
- collections, creating, 1022-1023**
- Collective Client Monitoring, 832-837**
- collectors. See ACS Collector Component**
- Collect\_Mailbox\_Statistics script**
  - parameters, 1302
- Collect\_Message\_Tracking\_Log\_Statistics script**
  - parameters, 1303
- Collect\_Public\_Folder\_Statistics script**
  - parameters, 1302-1303
- color, tuning alerts, 718-719
- COM (Component Object Model), 472**
- command notification, 1015-1016**
- Command Shell, 76, 1026-1029**
  - finding overrides, 712-714
  - online information, 1316
  - Operations Manager, 221
- command-line interface, 73**
  - installing databases from, 81
  - PowerShell, 132-134
- communication**
  - low bandwidth, 429-430
  - protocols, list of, 108-110
  - security, firewalls, 529
    - agents, 532-533
    - configuring proxy settings, 534
    - ports, 530-532
    - in SNMP, 846-848, 864
- community names, 846, 851**
- company knowledge, 339, 699**
- Compaq MIBs, 850**
- comparisons, new hardware/same hardware migrations, 285**
- complex configurations, 425**
- complex database clusters, installing, 452-454**
- complexity testing in proof of concept, 193**
- compliance regulations, online information on, 740**
- Component Object Model (COM), 472**
- components, 100**
  - ACS Collector Component, 227-228
  - ACS Database Server Component, 227
    - adding, 944
  - AEM, installation, 268-269, 271
  - Data Warehouse Component, 226-227
  - DEM, 800
  - Gateway Server Component, 224-225, 266-267

- installation, 234-235
  - ACS, 262-266
  - multiple-server Operations Manager, 241
  - order of, 240
  - reporting, 257-262
  - security accounts, 239
  - single-server Operations Manager, 241
  - software requirements, 239-240
  - Windows, 236
- management, installation, 256
- Management Server Component, 224
- MOM, 280
- Operations Database Component, 225-226
- Operations Database Server, installation, 242-248
- Operations Manager, 213
- planning, 203
  - ACS, 206-208
  - AEM, 211
  - Gateway Server Component, 208
  - managing agents, 208
  - reporting/trending, 204-206
  - Web Console Server, 212
- Reporting Server Component, 225
- RMS, installation, 249-256
- virtualization, 229-231
- Web Console Component, 228
- compression ratio, 429**
- computer accounts, provisioning, 1040-1041**
- Computer Discovery account, 499**
- computer discovery, scheduling, 372-373**
- computer group class, 70**
- computer groups, 70, 1017-1018**
- Computers global view, personalizing, 345-346**
- condition detection module type, 127, 602, 608**
- conditions, 651, 1021**
- Config Service account, 79, 107, 496-499**
- config space settings (data warehouse), 546**
- ConfigMgr (System Center Configuration Manager 2007), 21, 393-394**
  - clients, monitoring, 801
  - features in, 55-56
  - System Center Essentials versus, 96
- configsvc\_users role, 502**
- configuration, 280, 425**
  - ACS collector, 752-755
  - ACS database, 752-755
  - advanced monitoring for websites, 912-919
  - agent proxying, 358
  - agents, 414
    - Active Directory integration, 386-391
    - agentless managed state, 380-382, 404-408
  - ConfigMgr, 393-394
  - defining failover, 414-416
  - deleting, 417-418
  - deployment, 385-386
  - discovery process, 370-371
  - Discovery Wizard, 395-400
  - Group Policy deployment, 391-392
  - imaging, 395
  - manual installation, 402-403
  - modifying approval process, 373-374
  - network devices, 384
  - PowerShell installation, 403-404
  - proxying, 511
  - queue files, 416-417
  - scheduling computer discovery, 372-373
  - SMS, 393-394
  - state management, 374, 378, 380
  - troubleshooting, 418-422
  - unknown state, 384
- authentication, 919
- availability, planning, 221-229
- baselines (Exchange 2003 management pack), 1246-1249
- CA (certificate authority), 517-519
- components
  - ACS, 206-208
  - Gateway Server Component, 208, 211
  - managing agents, 208
  - planning, 203
  - reporting/trending, 204-206
  - Web Console Server, 212
- discovering objects, 333-335
- event logs, 411



- front-end monitors (Exchange Services), 970
  - inventorying configurations, 590-591
  - management group validation, 304-305
    - Active Alerts view, 315-317
    - distributed application Diagram view, 311-313
    - distributed application Health Explorer, 309-311
    - distributed application Performance view, 314-315
    - distributed application PowerShell integration, 313-314
    - global views, 307-309
    - Operations console installation, 305-307
    - reporting function, 319-322
  - management pack integration, 323, 1220-1224
    - default management packs, 323-325
    - importing management packs, 326-332
    - selecting management packs, 326
  - notifications, 689-690
  - OLE DB synthetic transactions, 922-925
  - rules, 1135-1136
  - SDK accounts, 253
  - self-tuning thresholds, 673-675
  - Service Provider Mode (System Center Essentials), 1079-1080
  - SSL, 525
  - TCP port monitors, 930-933
  - user roles, 477-483
    - resetting Administrator roles, 483-485
    - troubleshooting, 483
  - virtualization, 229-231
  - watcher nodes, 906
- configuration data (Operations console), 342**
- configuration health monitors, 121**
- Configuration Manager, 21, 55**
- installing Operations console, 1023
  - integration with, 1022-1024
- Configuration service (Registry keys), 1280-1281**
- Configure Client Monitoring wizard, 811**
- ConfigureEventLogs utility, 411**
- connected management groups, 85, 146-147, 362, 431**
- advantages, 1100
  - establishing connections, 1101-1105
  - example, 1099-1100
  - overview, 1096-1097
  - planning deployment, 215
  - prerequisite tasks, 1103-1105
  - security, 1100
  - viewing connected data, 1106
- connecting management groups, 1096**
- connections**
- to HP-OVO, 1109-1110
  - network connectivity requirements, 144
  - to Operations console, 338-339
  - Operations Manager, planning, 219-221
  - ports, firewalls, 530-532
  - testing, 919
  - to Tivoli TEC, 1110, 1112
  - watcher nodes, 906-907
- connector framework, 85**
- connectors**
- management packs versus, 85
  - online information, 1318-1321
  - product connectors, 219-220
    - HP-OVO connections, 1109-1110
    - overview, 1107-1109
    - third-party connectors, 1112-1114
    - Tivoli TEC connections, 1110-1112
  - Service Manager, 1029
- Consecutive Values over Threshold monitor, 670**
- console errors, 339-341**
- console tasks, 71, 356, 613, 1018-1021, 1149-1153**
- consoles, 73-75, 102**
- Authoring console
    - creating classes, 1178-1181
    - creating unit monitors, 1182
    - overview, 1175-1177
  - installation, 249-256
  - Mobile console, 360
  - operating system requirements, 158-159

- Operations console, 130-132, 228, 704, 1144
  - Administration space, 357-362
  - Authoring space, 352-357
  - configuration data, 342
  - connections, 338-339
  - console errors, 339-341
  - editing company knowledge, 339
  - hardware requirements, 155
  - importing management packs, 326-329
  - installation, 305-307, 336-337
  - Monitoring space, 344-351
  - My Workspace space, 366-367
  - navigation panes, list of, 343-344
  - Reporting space, 362-365
  - where to run, 305, 335-336
  - without trusted authentication, 340-342
- reporting, 88
- views, AEM, 812-814
- Web console, 132
  - hardware requirements, 156
  - performance counters, 1269
  - refresh interval, 366
  - URL settings, 359
  - Web Page views in, 359
- Web Console Component, 228
- Web Console Server, 212
- contents of groups, listing, 354**
- context menu tasks for alerts, enabling, 1292**
- Continual Service Improvement (ITIL v3), 27**
- controllers. See domain controllers**
- converted management packs, 164, 292**
- converting**
  - management packs to XML, 90
  - MOM 2005 management packs, 619-621
- cook down, 128-129**
- copying installation media to file server, 332**
- core model, 594**
- Corporate Error Reporting, 799**
- costs**
  - of downtime, 21
  - end-user problems, client monitoring, 802-803
- counters. See performance counters**
- Crash Listener view, 814**
- crashes, 802**
  - cost of, 802
  - monitoring, 807-812
  - testing, 810
- Create a Unit Monitor Wizard, 676, 682**
- Create Rule Wizard, 650, 654, 1136**
- Create Run As Account Wizard, 489**
- Create User Role Wizard, 478**
- CREATE\_NEWKEY command line switch, 574**
- credentials**
  - Action accounts, modifying, 496
  - entering in untrusted domains, 338
  - Run As Accounts, 489
- CSV files, viewing in Microsoft Excel, 713**
- current logged-on user (Registry keys), 1291-1292**
- Custom Data Manager, 874**
- custom distributed applications, 1039**
- custom files, backing up, 542**
- custom management packs, 988, 1034**
- custom resolution states, creating, 716-718**
- custom SNMP monitors, 877-878**
  - creating, 894-901
  - SNMPUTIL.exe utility, 878-880
- custom SNMP rules, 877-878**
  - creating, 880-894
  - SNMPUTIL.exe utility, 878-880
- Customer Experience Improvement Program (CEIP), 254, 359, 798**
- customer gateways, failover, 1092-1093**
- customer network devices, monitoring with ROM, 1073**
- customer networks, 1082-1083**
  - customer sites, 1083
    - approving, 1085-1087
    - configuring custom and value-add features, 1089-1093
    - creating, 1084-1085
    - discovering customer computers and network devices, 1088-1090

- installing System Center Essentials, 1074
- configuration options, 1076-1078
- OpsMgr management groups, 1075-1076

#### customization

- Action accounts, 494
- distributed applications, 986
- error buckets, 816-819
- Line of Business Web application templates, 992-994
- migration, 278
- web addresses, 917

## D

- DA (Distributed Application, OpsMgr), 952-953**
- daily growth rate for ACS database, 779
- DAs (distributed applications), 940-941, 944, 947**
- dashboard view, creating, 347-349
- data flow, 86-88, 179
- Data Protection Manager 2007, 58-59**
- Data Reader account, 165, 500**
- data retention, 544**
  - ACS database, 553, 765
  - data warehouse database, grooming, 545-553
  - Operational database, grooming, 545
- data source module type, 126, 602, 608**
- Data Source Service DA, customizing, 984-986**
- data sources**
  - creating, 1203-1204
  - for monitors, 85
  - views, creating, 1204
- data tier (distributed applications), 950**
- data types, 129, 605, 607**
- data warehouse**
  - backing up, 541, 550-553
  - grooming, 545-553
  - for historical data, 48
  - moving, 567-569
  - promoting management server to RMS, 576

- security, 502-503
- sizing and capacity limitations, 184-187
- transferring data to, 89
- troubleshooting, 321-322

#### **Data Warehouse Action account, 487**

#### **data warehouse clusters, installing, 449-451**

#### **Data Warehouse Component, 226-227**

#### **Data Warehouse Internal Library, 375**

#### **Data Warehouse Library, 375**

#### **data warehouse server**

- hardware requirements, 155
- name, location of, 569
- Registry keys, 1281

#### **Data Warehouse SQL Authentication Action account, 487**

#### **Data Warehouse Write account, 165**

#### **Data Warehouse Write Action account, 499**

#### **database clustering, 82-83**

#### **database grooming settings, 358**

#### **database servers**

- clustering ACS database servers, 748
- moving
  - ACS database, 569-570
  - Data Warehouse database, 567-569
  - Operations database, 565-567
- operating system requirements, 157-158
- Registry keys, 1281

#### **database sizing spreadsheet, 187**

#### **databases. *See also* data warehouse**

- ACS database
  - configuring, 752-755
  - data retention period, 765
  - granting permissions on, 754-755
  - security settings, 756
  - size management, 778-780
  - system-level management, 765
- backups, 540
- complex database clusters, installing, 452-454
- DAs, adding to, 942
- documenting, 570
- on existing SQL Server databases, 152
- grooming, 545

- installing from command line, 81
- monitoring, 922-933
- naming, 80-81
- network bandwidth utilization, 145
- Operations Database Server, installation, 242-248
- restoring, 565
- security, 502-503
- sharing among management groups, 104
- space utilization, 629
- system versus user databases, 540

#### **datasets, 548-550**

**dbcreatewizard.exe tool, 453-454**

**dbmodule\_users role, 502**

**DDNS (Dynamic DNS), 1067**

#### **debugging**

- AeDebug, applying, 811
- alerts, 1309

#### **decommissioning**

- MOM 2005 environments, 296
- original monitoring solutions, 280

**Default Action account, 487**

**Default Management Pack, 90, 323-325, 375, 611-612**

**default ports, list of, 108-110**

#### **defining**

- agent failover, 414, 416
- overrides, 706-707
- roles, scopes, 480

**defragmenting disks, 1035-1036**

#### **deleting**

- Active Directory Integration, 391
- agentless systems, 1309
- agents, 417-418
- certificates, 519
- management packs, 1142-1143
- Operations Manager, 271-272

**Dell management pack, 1259-1260**

**Dell OpenManage, 871**

**Dell Server Management Pack, 1116**

**Delta Threshold monitor, 670-671**

**DEM (Microsoft System Center Desktop Error Monitoring), 800**

#### **dependencies**

- importing management packs, 327, 330
- of management packs, design stage (deployment planning), 164
- removing, 611-612
- service dependencies in assessment documents, 140

**dependency checks (management packs), 597**

**dependency monitors, 119-122, 604**

**dependency rollup monitors, 121, 682**

**deployment. See also deployment planning**

- of ACS, steps in, 740-741
- AEM policies, 807-812
- agentless monitoring, 404-405
- agents, 385-386
  - Active Directory integration, 386-391
  - ConfigMgr, 393-394
  - Discovery Wizard, 395-400
  - Group Policy, 391-392
  - imaging, 395
  - manual installation, 402-403
  - PowerShell installation, 403-404
  - SMS, 393-394
  - troubleshooting, 418-422

#### **components**

- ACS, 206-208
- AEM, 211
- Gateway Server Component, 208
- managing agents, 208
- planning, 203
- reporting/trending, 204-206
- Web Console Server, 212
- multihomed, planning, 214
- report models, 1206

**Deployment Guide, 1107**

**deployment planning, 137-138. See also deployment**

- ACS components, 747-752
- ACS collectors, number of, 750-751
- clustering ACS database servers, 748
- reporting services integration, 749
- security boundary, creating, 748-749
- SQL Server 2005 Standard versus Enterprise editions, 751

assessment stage, 139-141, 425

design stage

agent deployment, 165

business requirements, 141

management groups, 141-148

management packs, 164

monitored servers, 164

multiple-management group design  
sample, 198-200

multiple-server configuration example,  
174-178

notifications, 165

reporting, 165

security accounts, 164-165

server components, 148-156

single-management group design  
sample, 198-199

single-server design sample, 196-197

single-server monitoring configuration  
example, 167-171

sizing and capacity limitations, 178-189

software requirements, 156-163

System Center Capacity Planner  
(SCCP), 166

two-server configuration example,  
170-174

user applications, 164

gateway servers

approving, 435-436

authentication, 432-434

redundancy, 436-437

implementation stage, 191, 194

maintenance stage, 195

management packs, 621

exporting, 634-635

importing, 636-640

order of implementation, 621-622

troubleshooting, 631-634

tuning, 622-631

management server configurations, 425

multihomed deployments, 431-433

multilocation deployments, 426-429

multiple management groups, 430-431

pilot stage, 191-194

proof of concept stage, 190-193

redundancy, 437-440

ACS clusters, installing, 451-452

AEM clusters, installing, 454

clusters, 440-441

clusters, installing, 441-442

clusters, testing failover, 442-443

complex database clusters, installing,  
452-454

data warehouse clusters, installing,  
449-451

Operations database clusters, installing,  
447-448

options for, 438-439

reporting server clusters, installing,  
455-457

RMS clusters, installing, 457-467

SQL Server 2005 clusters, installing,  
443-447

**deprovisioning**

applications, 1039-1040

user accounts, 1040-1041

**design stage (deployment planning)**

agent deployment, 165

business requirements, 141

management groups, 141-148

management packs, 164

monitored servers, 164

multiple-management group design sample,  
198-200

multiple-server configuration example,  
174-178

notifications, 165

reporting, 165

security accounts, 164-165

server components, 148-156

single-management group design sample,  
198-199

single-server design sample, 196-197

single-server monitoring configuration  
example, 167-171

sizing and capacity limitations, 178-189

software requirements, 156-163

System Center Capacity Planner  
(SCCP), 166

- two-server configuration example, 170-174
- user applications, 164
- design validation in proof of concept, 192**
- detailed logging, enabling on ACS forwarders, 776**
- detection monitors**
  - probe-based (SNMP), creating, 895-898
  - trap-based (SNMP), creating, 898-901
- developing management packs, 1141**
- Device Management node (Administration space), 357-358**
- devices, networks, 384**
- DFS (Distributed File System) for AEM cluster installation, 454**
- diagnostic tasks, 1008-1010**
  - console tasks and, 1019-1021
  - creating, 1009-1012
- diagnostic tracing, 645**
- diagnostics, 119, 601-604**
- Diagram view**
  - Active Directory Topology Root, 962
  - for distributed applications, 311-313
  - Operations Manager Management Group, 956, 958
- Director, 871**
- Director Management Pack (IBM), 1118**
- directories. See Active Directory**
- disabling**
  - attributes, 355
  - events, 627
  - monitoring with maintenance mode, 727-730
  - monitors, 623, 629
  - rules, 356, 623, 629
  - version checking in Registry, 66
- disaster recovery, 586**
  - from downed RMS, 589
  - inventorying OpsMgr configuration, 590-591
  - with log shipping, 588
  - from total loss, 586-587
  - virtualization, 589
- DisconnectThreshold value (ACS collector performance), 774**
- discoveries, 119, 603-604**
- discovering**
  - agents, 370-373
  - components (SQL Server management pack), 1250-1251
  - customer computers and network devices, 1088, 1090
  - network devices, 850-864
    - adding with Discovery Wizard, 853-856
    - adding with PowerShell, 857-859
    - changing proxy agents, 859-863
    - preparations for, 850-852
    - SNMP polling conversation contents, 864
  - objects, 333-335
- discovery objects, 355**
- discovery overrides, 610**
- discovery rules, 872**
- Discovery Wizard, 294, 333-335, 371**
  - adding network devices, 853-856
  - agentless monitoring, deploying, 404-405
  - agents, deploying, 395-400
- disk backups, 1037**
- disk defragmentation, 1035-1036**
- disk performance, 412, 469-470**
- Distributed Application Designer, 943, 946, 986**
- Distributed Application Designer Library, 375**
- distributed application Diagram view, 311-313, 947**
- distributed application Health Explorer, 309-311**
- distributed application Performance view, 314-315**
- distributed application PowerShell integration, 313-314**
- distributed application services, creating, 352-353**
- distributed applications, 940, 949-950, 1038**
  - Active Directory Topology Root, 954, 958-959
    - Diagram view, 962
    - in-line tasks, 961
    - viewing health with monitors, 959-960
  - business logic tier, 950
  - custom distributed applications, 1039
  - customizing, 986

- data tier, 950
- Exchange Service, 954, 962-964
  - Availability Monitor, 967-970
  - configuring front-end monitors, 970
  - Exchange Service DA, 965-966
  - Exchange views, 964-965
- forests, 958
- health models, creating, 986-989
  - Blank templates, 998-1002
  - Line of Business Web application templates, 988-994
  - Messaging templates, 994-996
  - Terminal Services Farm templates, 996-998
- monitoring specific objects, 992
- Operations Manager Management Group, 954
  - Alerts view, 955-956
  - Diagram view, 956-958
  - Health Explorer, 954-955
  - Performance view, 955-956
- OpsMgr as, 1038
- predefined distributed applications, forests, 958
- provisioning, 1039-1040
- release cycles, 950-952
- SDK versus, 987
- software containers, 950
- user-interface tier, 950
- Distributed Applications state global view, 309**
- Distributed File System (DFS) for AEM cluster installation, 454**
- distributed management, 38**
- DMZs**
  - Gateway Server Component, monitoring agents, 208
  - preparing operations manager for ROM, 1070
- DNS**
  - preparing operations manager for ROM, 1065-1067
  - troubleshooting, 624
- documentation**
  - databases, 570
  - migration, 280

**Domain and Built-in Administrators Changes report, 785**

**Domain Controller Security Policy, 742-743**

**domain controllers, 390**

- enabling certificate support, 528
- encryption, 529
- minimum security log settings, 745

**Domain Security Policy, 741-743**

**domains**

- accounts, updating, 495
- multiple, planning, 216-218
- non-trusted, OpsMgr, 504-506
- properties, Windows, 236
- untrusted domains, entering credentials, 338

**Double Threshold monitor, 671**

**downloading resource kit utilities, 730**

**downtime, cost of, 21**

**DPM (Data Protection Manager) 2007, 58-59**

**Dr. Watson, 798**

**drive configurations**

- System Center Essentials, 169
- two-server configuration example, 174

**drivers (ACS), permitting, 395**

**DSI (Dynamic Systems Initiative), 22-25**

**dwsynch\_users role, 502**

**dynamic computer groups, populating with Health Service watchers, 1018**

**Dynamic DNS (DDNS), 1067**

**Dynamic level (IO Model), 34**

**dynamic membership, 1017**

**Dynamic Systems Initiative (DSI), 22-25**

## E

**e-commerce sites, cost of downtime, 21**

**E2E (end-to-end) service management, 36, 949**

**Eclipse migration case study, 288-298**

**Edge Transport role (Exchange 2007), 1031**

**editing**

- company knowledge, 339
- knowledge in management packs, 598-599
- MOMAuth.xml files, 484

**Effective Configuration Viewer, 731-733****elements (of management packs), 605-606**

- class types, 606
- console tasks, 613
- data types, 607
- folders, 614
- module types, 607-608
- overrides, 608-611
- presentation types, 612-613
- relationship types, 607
- report parameters, 614
- reports, 614
- schema types, 607
- templates, 612-613
- unit monitor types, 608
- views, 614

**email, 939**

- flow, monitoring, 939
- forwarding alerts, 690
- security least privilege, 1067
- sending reports, 366, 1215-1216

**email format, testing, 690****email-enabled user accounts, creating, 1032****embedding tasks in alert details, 688****Enable Audit Collection task, running, 760-762****enabling**

- ACS forwarders, 760-762
- ACS with PowerShell, 763
- certificate-based ACS forwarders, 782
- context menu tasks for alerts, 1292
- detailed logging on ACS forwarders, 776
- encryption, 529
- failover for ACS forwarders, 780-782
- log shipping, 588
- permitted SNMP managers, 851
- SNMP, 851
- trap sending, 852

**encryption, enabling, 529****encryption keys (RMS)**

- backing up, 570-572
- creating, 574

**encryption keys (SRS), backing up, 584-585****end-to-end (E2E) service management, 36, 949****enterprise CA, 513**

- certificates
  - creating templates, 513
  - exporting, 514-515
  - requesting, 513-514
- versus standalone CA, 1067-1069

**Enterprise Health Monitoring, 971-972**

- Internet Explorer Service templates, 973
  - creating web applications, 973-976
  - creating Windows Internet Explorer Service DA, 976-980
- Windows Explorer Data Source Service templates, 980
  - creating OLE DB Data Sources, 980-981
  - creating Windows Explorer Data Source Service DA, 982-984
  - customizing Data Source Service DA, 984-986

**Enterprise Master Hoster, 1060-1062**

- Audit Collection Services, 1063
- customers-per-gateway capacity, 1063-1065
- redundant configurations, 1063

**enterprise OML, 159****environment, adapting to, 1008, 1035**

- Active Directory integration, 1033-1034
- Capacity Planner integration, 1024-1025
- computer groups, 1017-1018
- Configuration Manager integration, 1022-1024
- console tasks, 1018-1021
- custom management packs, 1034
- diagnostic tasks, 1008-1012
- distributed applications, 1038-1040
- Exchange 2007 integration, 1031-1033
- notifications, 1015-1016
- PowerShell integration, 1026-1029
- recovery tasks, 1008-1010, 1013-1014
- security adaptations, 1041-1042
- servers, provisioning, 1042-1045
- Service Manager integration, 1029
- SharePoint integration, 1029-1031
- system maintenance, 1035-1038
- user accounts, provisioning, 1040-1041



Virtual Machine Manager integration,  
1025-1026

VMWare integration, 1034

**error messages**

availability after moving databases, 567  
when importing management packs, 638

**error reports, sending to Microsoft, 247**

**errors**

Application Error Group view, 813  
applications, events, 812  
buckets, customizing, 816-818  
CER, 799-800  
console errors, 339-341  
groups, Top Error Groups report, 821-823  
surveys, 818-819  
Windows Error Reporting, 798-799

**ES7000 Management Pack (Unisys), 1118**

**Essentials. See System Center Essentials**

**ESX monitoring, 1130**

**evaluation copies**

System Center Essentials, 94  
OpsMgr 2007, 92

**Event Counts by Computer report, 783**

**Event Counts report, 783**

**Event ID 26319, 497**

**event latency, increasing, 776**

**event logs, 16**

notification, lack of, 16-17, 40-43  
Registry keys, 1287-1288

**event rules, creating trap-based event rules  
(SNMP), 886-888**

**event-based alert-generating rules, 880**

**event-based collection rules, 880, 888-891**

**event-based event-generating rules, 880**

**event-processing rules, 872**

**EventCombMT.exe utility, 64**

**events**

applications, errors, 812  
disabling, 627  
forwarding, 207  
logs, agent management, 410-412  
reports, 627

**eXc software, 1121-1122**

**Excel, viewing CSV files, 713**

**Exchange 2003 management pack**

configuring baselines, 1246-1249  
installation, 1236-1237  
OWA logon failure, 1244-1246  
troubleshooting, 1237  
tuning and alerts, 1237-1244

**Exchange 2007**

importing, 938  
integration with, 1031-1033  
monitoring, 933-935, 939-940  
user accounts, creating, 1032

**Exchange 2007 Management Pack, 964**

**Exchange management pack script parameters,  
964, 1300-1303**

**Exchange Server 2003 management pack,  
tuning, 723-724**

**Exchange Server Management Pack**

Configuration Wizard, online information, 1313

**Exchange Service DA, 965-966**

**Exchange Services, 954**

distributed applications, 962-964  
Availability Monitor, 967-970  
configuring front-end monitors, 970  
Exchange Service DA, 965-966  
Exchange views, 964-965

**expertise, lack of, 18**

OpsMgr 2007 solutions to, 48-50

**exporting**

certificates, 514-515  
management packs, 577, 634-635  
reports, 365

**Extensible Markup Language. See XML**

**extensible monitoring, 598**

**external sites, monitoring, 999**

**extracting management pack packages, 636**

## F

**facility values, 1137**

**failback, 441**

**failover, 441**

- for ACS forwarders, enabling, 780-782
- agents, defining, 414-416
- customer gateways, 1092-1093
- of gateway servers, 436
- testing, 442-443

**failover partners, 426**

**failover servers for agents, 426-427**

**failures, 14**

**false alarms, 19, 52-54**

**farms, 996**

**File Replication Service (FRS), 512**

**file server, copying installation media to, 332**

**files**

- .CAB, 811
- MOMAuth.xml, editing, 484
- .MP extension, 1164

**finding**

- overrides, 712-715
- rules/monitors in Operations console, 703-706

**firewalls, 529**

- agents, 532-533
- Group Policy, 258
- outbound, 1079
- ports, 530-532
- preparing operations manager for ROM, 1070
  - installing Service Provider management pack, 1072-1073
  - ISA Server, 1070-1071
  - publishing rules, 1071-1072
  - proxy settings, configuring, 534

**Flexible Single Master Operations (FSMO), 222**

**flow of email, monitoring, 939**

**folders, 614**

**Forefront, security, 1140**

**Forensic category (audit reports), 784**

**forests, predefined distributed applications, 958**

**forwarders. See ACS forwarders**

**forwarding**

- alerts by email, 690
- events, 207

**FQDNs (Fully Qualified Domain Names), 503, 1057**

**free space, tracking, 194**

**front-end monitors, configuring (Exchange Services), 970**

**FRS (File Replication Service), 512**

**FSMO (Flexible Single Master Operations), 222**

**full backups, 555**

**full recovery, 554**

**Fully Qualified Domain Names (FQDNs), 503, 1057**

**functionality changes in OpsMgr 2007, 71-88**

- ACS, 86
- Active Directory integration, 79-80
- Agentless Exception Monitoring, 72
- agents, 83
- client monitoring, 85
- Command Shell, 76
- connected management groups, 85
- connector framework, 85
- consoles, 73-75
- data flow, 86-88
- database clustering, 82-83
- database naming, 80-81
- Health Explorer, 75-76
- maintenance mode, 83
- model-based management, 71
- monitoring engine, 83-85
- notifications, 83
- Registry keys, 81
- role-based security, 77-78
- Run As Accounts, 79
- Run As Profiles, 78
- self-tuning thresholds, 83
- server components, 81-82
- service-oriented monitoring, 71-72
- services, 79
- SNMPv2 support, 76
- WS-Management support, 76

**functionality requirements in assessment documents, 140**

## G

**Gateway Action account, 501-502**

**Gateway Approval Tool, permissions needed, 436**

**Gateway Server Component, 208, 211, 224-225, 1054-1055**

installation, 266-267

online information, 1306

**gateway servers, 82, 104, 224, 435**

approving, 435-436

applying, 504, 506

authentication, 432, 434

hardware requirements, 152-153

management group design, 146

reducing network traffic with, 429

redundancy, 436-437

**GC (Global Catalog) servers, positioning, 725**

**generic reports, 364-365**

**Get messages (SNMP), 846-847**

**Get-UserRole cmdlet, 480**

**Global Catalog (GC) servers, positioning, 725**

**global views, 307-309**

**GPMC (Group Policy Management Console), 744, 807**

**GPO (Group Policy Object), 412, 744**

**granting permissions on ACS database, 754-755**

**grooming**

ACS database, 553

data warehouse database, 545-553

Operational database, 545

ROM, 1076-1077

settings for, 358

**Group override, 610**

**Group Policy**

deployment, 391-392

firewalls, 258

**Group Policy Management Console (GPMC), 744, 807**

**Group Policy Modeling Wizard, 744**

**Group Policy Object (GPO), 412, 744**

**groups**

Administrator role, resetting, 483-485

Application Error Group view, 813

computer groups, 1017-1018

connected management deployment, planning, 215

creating, 353

errors, Top Error Groups report, 821-823

listing contents of, 354

management groups, 1098

multihomed agents, 409-410

System Error Group view, 814

targeting rules/monitors, 665-666

## H

**Hambrook, Jonathan, 1130**

**hangs**

cost of, 802

monitoring, 807, 809-812

testing, 810

**hardware**

migration

case studies, 288-298

new hardware, 284-288, 297-298

same hardware, 281-283, 288-296

requirements

ACS Collector, 155

ACS database servers, 155

ACS Forwarder, 155

agents, 156

comparison chart, 92-93

data warehouse servers, 155

gateway servers, 152-153

management servers, 151-152

multiple-server configuration example, 175

Operations console, 155

Operations database, 152-154

reporting servers, 154

Root Management Server (RMS), 149-150

- System Center Essentials, 169
  - two-server configuration example, 173
  - Web console, 156
- sharing, 80
- hardware management packs, importing, 865-872, 874-877**
- Health Explorer, 40, 75-76, 350-351, 624, 626**
  - for distributed applications, 309-311
  - Operations Manager Management Group, 954-955, 958
- Health Internal Library, 375**
- Health Library, 375**
- health models, 600**
  - distributed applications, creating, 986-989
  - Blank templates, 998-1002
  - Line of Business Web application templates, 988-994
  - Messaging templates, 994-996
  - Terminal Services Farm templates, 996-998
- explained, 115-117
- monitors in, 120
- health rollups, IIS management pack, 1255**
- Health service, 69, 79**
  - explained, 105-106
  - performance counters, list of, 1262
  - Registry keys, 1288-1291
  - restarting, 1014
- Health Service account, 501**
- Health service lockdown tool, 525-526**
- Health Service Management Group, list of performance counters, 1262-1264**
- Health Service watchers, populating dynamic computer groups, 1018**
- health state, 69**
- heartbeat settings**
  - agents, 358-359
  - reducing network traffic, 430
- help information for PowerShell, 1028**
- Hewlett-Packard ProLiant Servers Base, 873**
- Hewlett-Packard ProLiant Servers SNMP Management Pack, 873**
- Hewlett-Packard Servers Core Library, 873**
- hidden shares, creating, 463**
- high availability**
  - with database clustering, 82-83
  - planning configurations, 221-222, 224-229
- historical information, lack of, 17, 44-49**
- history of OpsMgr 2007, 64-65**
- hives (Registry), 1272**
- HKEY\_CLASSES\_ROOT (HKCR) Registry key, 1271**
- HKEY\_CURRENT\_USER (HKCU) Registry key, 1271**
- HKEY\_CURRENT\_CONFIG (HKCC) Registry key, 1272**
- HKEY\_LOCAL\_MACHINE (HKLM) Registry key, 1271**
- HKEY\_USERS (HKU) Registry key, 1271**
- horizontal scaling, 1042-1043**
- Hourly Event Distribution report, 783**
- HP OpenView, 871**
- HP Servers Management Pack for Operations Manager 2007, 871-877, 1114-1116**
- HP Systems Insight Manager (HP-SIM), 871**
- HP-OVO, connecting to, 1109-1110**
- HP-SIM (HP Systems Insight Manager), 871**
- HP/Compaq MIBs, 850**
- Hub Transport role (Exchange 2007), 1031**
- hybrid approach, new hardware/same hardware migrations, 286**

## I

- IBM Director, 871**
- IBM Director Management Pack, 1118**
- IBM Tivoli, 871**
- icons, 120**
- ID attributes (management pack elements), 605**
- identifiers, management packs, 1165**
- IIS management pack, 1254-1255**
- IIS metabase, backing up, 542**
- Image Library, 375**
- images, 613**
- imaging, 395**

**implementation**

AEM, 805-812

of audit policies, 763-766

**implementation order for management packs, 621-622****implementation stage (deployment planning), 191, 194****Import Management Packs dialog box options, 327****importing**

built-in templates into Local Security Policy, 743

certificates on ROM servers, 1069-1070  
Exchange, 938

hardware management packs, 865-877

management during installation, 594

management packs, 326-332, 636-640

with Operations console, 636-638

with PowerShell, 638

verifying installation, 639-640

**in-line tasks (Active Directory Topology Root), 961****increasing**

event latency, 776

queue size, 633

**Information Technology (IT) systems, 906****Information Technology Infrastructure Library (ITIL), 1049****Infrastructure Optimization (IO) Model, 22****installation**

ACS, 262, 264, 266

ACS clusters, 451-452

ACS reports, 756-757

of Active Directory management pack, 1229-1230

AEM, 268-269, 271

AEM clusters, 454

agents, 294

Active Directory integration, 386-391

agentless managed state, 380-382, 404-408

ConfigMgr, 393-394

deployment, 385-386

discovery process, 370-371

Discovery Wizard, 395-397, 399-400

Group Policy deployment, 391-392

imaging, 395

manual installation, 402-403

modifying approval processes, 373-374

modifying pending actions, 412-413

network devices, 384

PowerShell installation, 403-404

scheduling computer discovery, 372-373

SMS, 393-394

state management, 374, 378, 380

troubleshooting, 418-422

unknown state, 384

ASP.NET, 249

CER, 799

**certificates**

ACS collectors, 528

ACS forwarders, 527-528

enabling certificate support, 528

encryption, 529

of clusters, 441-442

complex database clusters, 452-454

consoles, 249-251, 253-254, 256

data warehouse clusters, 449-451

databases from command line, 81

of Exchange 2003 management pack, 1236-1237

Gateway Server Component, 266-267

of IIS management pack, 1254-1255

importing management packs, 594

management packs, 639, 1220-1224

management servers, 256

**migration**

case studies, 288-298

troubleshooting, 299-300

multihomed agents, 432

multiple-server Operations Manager, 241

new hardware migrations, 284-288, 297-298

OOMADS, 285

of Operations console, 305-307, 1023

Operations database clusters, 447-448

Operations Database Server, 242-248

- order of, 240
- planning, 234
- prerequisites, 234-235
  - Operations console, 336-337
  - security accounts, 239
  - software requirements, 239-240
  - Windows, 236
- reporting components, 257-260, 262
- reporting server clusters, 455-457
- RMS, 249-251, 253-254, 256
- RMS clusters, 457-458, 460-467
- RWW, Service Provider Mode (System Center Essentials), 1080-1082
- same hardware migrations, 281-283, 288-296
- Service Provider management pack (ROM), 1072-1073
- SetupOM.exe, 234
- single-server Operations Manager, 241
- SQL Server 2005 clusters, 443-447
- SQL Server management pack, 1249-1250
- starting clean, 278-281
- System Center Essentials on customer networks, 1074
  - configuration options, 1076-1078
  - OpsMgr management groups, 1075-1076
- troubleshooting, 273-275
- Xian IO, 1126
- installation class, 70**
- installation kits for HP hardware management packs, 873**
- installation media, 332**
- Instance Group Library, 375**
- instance space settings (data warehouse), 546**
- integration**
  - Active Directory, 218-219, 386-391, 473
  - agentless managed systems, 404-405
  - of management packs, 323
    - default management packs, 323-325
    - importing management packs, 326-332
    - selecting management packs, 326
  - of OpsMgr 2007, 140
- integration scenarios for ACS reports, 758-760**

- Internet Explorer, viewing XML files in, 1166**
- Internet Explorer Service templates (Enterprise Health Monitoring), 973**
  - creating web applications, 973-976
  - creating Windows Internet Explorer Service DA, 976-980
- interoperability**
  - connected management groups
    - advantages, 1100
    - establishing connections, 1101-1105
    - example, 1099-1100
    - overview, 1096-1097
    - prerequisite tasks, 1103-1105
    - security, 1100
    - viewing connected data, 1106
  - integration with other system center applications, 1138-1139
  - management packs, 1114
    - Citrix Presentation Server Management Pack, 1118-1119
    - Dell Server Management Pack, 1116
    - HP Server Management Packs for OpsMgr 2007, 1114-1116
    - IBM Director Management Pack, 1118
    - Unisys ES7000 Management Pack, 1118
  - non-Windows systems, managing
    - eXc software, 1121-1122
    - Jalasoft Xian IO, 1123-1127
    - nworks VMware Management, 1128-1130
    - overview, 1120-1121
    - Quest Management Xtensions, 1128
    - Syslog message capturing, 1135-1137
    - TCP port monitoring, 1131-1135
  - notifications, 1119-1120
  - overview, 1095-1096
  - product connectors
    - HP-OVO connections, 1109-1110
    - overview, 1107-1109
    - third-party connectors, 1112-1114
    - Tivoli TEC connections, 1110, 1112
- inventorying OpsMgr configuration, 590-591**
- IO Model (Infrastructure Optimization), 22, 31-34, 1312**

**ISA (Internet Security and Acceleration) Server, 1070-1071**

islands of information, problems with, **15-16, 37-39**

**ISO 20000, 31**

**IT distributed application problems, 952**

**IT Service Management (ITSM), 26**

**ITIL (IT Infrastructure Library), 26-31, 1049**

explained, 26-28

MOF relationship with, 31

version 3, 26-27

**ITSM (IT Service Management), 26**

**IT systems, 906**

## J–K

**Jalasoft Xian IO, 1123-1127**

**Kangas, Stephen, 65**

**Kerberos authentication, 217, 432**

keys. *See* Registry keys

**Kleptomania, 698**

**knowledge**

adding to alerts, 699-703

in management packs, 598-599

## L

**Language Types section (management pack schema, 1164**

languages, management group design, 146.  
*See also* XML

**latency, increasing event latency, 776**

**launching batch files with timed commands, 663-665**

**learning rate, 674**

**libraries, 594**

**licensing OML (Operations Management License), 159-162**

**LicensingWizard.msi, 279**

**Line of Business Web application templates, 988-990**

customizing, 992-994

Object Picker, 990-992

**linked reports, creating, 1198-1202**

**listing management packs, 641-642**

**Live Maps (Savision), 1123**

**load balancing with multiple management servers, 426-427**

**LOB applications, monitoring, 928-933**

**Local Security Policy, 741-743**

**Local Service accounts, 495**

**log file monitor, 679-680**

**log files, 16 322**

**log shipping, 448-449, 588**

**Logon Counts of Privileged Users report, 783**

**logons (MAPI), monitoring, 939**

**logs**

events, agent management, 410-412

security, 410

transaction logs

backups, effect on, 561

truncating, 556, 560, 562-563

**low-bandwidth communication, 429-430**

**low-privileged accounts, 493-494**

## M

**machines, monitoring client, 800-801**

**Mailbox role (Exchange 2007), 1031**

**maintenance, 1035**

**maintenance mode, 83, 727-730**

online information, 1309

settings, 349-350

**maintenance stage (deployment planning), 195**

**maintenance windows in ConfigMgr 2007, 55**

**MaintenanceSetting table (data warehouse), 546**

**managed devices, 846**

**Managed Service Providers (MSPs), 966**

**management, 22. See also management packs**

agent-managed systems, monitoring clients, 828-842

agents, 410

agentless managed state, 380-382, 404-408

configuring settings, 414

defining failover, 414, 416

deleting, 417-418

disk performance, 412

event logs, 410-412

multihomed, 409-410

network devices, 384

pending action, 412-413

queue files, 416-417

state, 374, 378, 380

unknown state, 384

components

ACS, 206-208

AEM, 211

agents, 208

Gateway Server Component, 208

planning for additional, 203

reporting/trending, 204-206

Web Console Server, 212

connected group deployment, planning, 215

installation, 234

ACS, 262, 264, 266

AEM, 268-269, 271

Gateway Server Component, 266-267

multiple-server Operations Manager, 241

Operations Database Server, 242-248

order of, 240

prerequisites, 234-235

reporting components, 257-260, 262

security accounts, 239

single-server Operations Manager, 241

software requirements, 239-240

Windows prerequisites, 236

Microsoft's strategy, 22

DSI, 22-25

IO Model, 31-34

ISO 20000, 31

ITIL, 26-31

MOF, 26-31

non-Windows systems

eXc software, 1121-1122

Jalasoft Xian IO, 1123-1127

nworks VMware Management, 1128-1130

overview, 1120-1121

Quest Management Xtensions, 1128

Syslog message capturing, 1135-1137

TCP port monitoring, 1131-1135

Operations Manager

agents, 229

deleting, 271-272

planning connections, 219-221

RMS, 203, 222, 224, 249-256

servers

Action account, 492-495

adding, 503

configuring proxy settings, 534

installation, 256

modifying credentials, 496

mutual authentication, 503-507, 511

**Management Group ODR Report, 825****management groups**

adding network devices, 853-859

connected management groups, 362, 431

advantages, 1100

establishing connections, 1101-1105

example, 1099-1100

overview, 1096-1097

prerequisite tasks, 1103-1105

security, 1100

viewing connected data, 1106

connections, 338

design stage (deployment planning), 141-148

architectures, 146-148

dedicated ACS management group, 143

gateway servers, 146

installed languages, 146

network environment, 144

physical locations, 143



- processing power requirements, 146
- production and test environments, 143
- security model, 143
- separating administrative control, 142
- support limits, 142
- explained, 98-100
- Health Service Management Group, list of performance counters, 1262-1264
- multiple management groups, 176-177, 188-189, 430-431
- naming, 100, 144
- scalability, 187-188
- settings in Administration space, 358-359
- sharing resources among, 104
- sizing and capacity limitations, 180-181, 430
- tiered management groups, 1098-1099
- validation, 304-305

- Active Alerts view, 315-317
- distributed application Diagram view, 311-313
- distributed application Health Explorer, 309-311
- distributed application Performance view, 314-315
- distributed application PowerShell integration, 313-314
- global views, 307-309
- Operations console installation, 305-307
- reporting function, 319-322

#### **Management Information Base, 848**

**Management Pack node (Administration space), 361**

**Management Pack Objects node, 354-357**

**management pack packages, extracting, 636**

**management pack schema, explained, 117-119**

**management pack templates, 352**

**management packs, 48-51, 647, 1114**

- Active Directory management pack, 386, 1033, 1229-1230
  - AD\_Client\_Connectivity script parameters, 1299
  - AD\_Client\_GC\_Availability script parameters, 1300
  - AD\_Client\_PDC\_Response script parameters, 1300

- AD\_Database\_and\_Log script parameters, 1296-1297

- AD\_Essential\_Services\_Running script parameters, 1299

- AD\_General\_Response script parameters, 1297

- AD\_Global\_Catalog\_Search\_Response script parameters, 1297

- AD\_Op\_Master\_Response script parameters, 1298-1299

- AD\_Replication\_Monitoring script parameters, 1296

- tuning and alerts, 724-725, 1230-1235

**AKM file format, 1163**

**backing up, 542**

- with Operations console, 580-582

- with PowerShell scripts, 577-580

**Baseline Security Analyzer management pack, 1036**

**changes in, 89-90**

**Citrix Presentation Server Management Pack, 1118-1119**

**clients, 798**

**comparison of creation techniques, 1225**

**connectors versus, 85**

**conversion, 90, 292**

**creating with Authoring console**

- classes, 1178, 1180-1181

- overview, 1175-1177

- unit monitors, 1182

**creating with Operations console**

- console tasks, 1149-1153

- monitors, 1143-1149

- options, 1160

- overview, 1141-1143

- rules, 1156-1159

- views, 1154, 1156

**creating with Silect MP Studio, 1183-1188**

**custom management packs, 988, 1034**

**customer names, 1092**

**data types, 605**

**database sizing and, 182**

**Default management pack, override storage location, 611-612**

- definition, 1143
- deleting, 1142-1143
- Dell management pack, 1259-1260
- Dell Server Management Pack, 1116
- dependency checks, 597
- deployment planning, 621
  - order of implementation, 621-622
  - tuning, 622-631
- design stage (deployment planning), 164
- diagnostic tracing, 645
- diagnostics and recovery, 601-602
- for earlier OpsMgr versions, 617
- elements of, 605-606
  - class types, 606
  - console tasks, 613
  - data types, 607
  - folders, 614
  - module types, 607-608
  - overrides, 608-611
  - presentation types, 612-613
  - relationship types, 607
  - report parameters, 614
  - reports, 614
  - schema types, 607
  - templates, 612-613
  - unit monitor types, 608
  - views, 614
- Exchange 2003 management pack
  - configuring baselines, 1246-1249
  - installation, 1236-1237
  - OWA logon failure, 1244-1246
  - troubleshooting, 1237
  - tuning and alerts, 1237-1244
- Exchange 2007 management pack, 1032-1033
- Exchange management pack, 933-935, 939-940
  - Collect\_Mailbox\_Statistics script parameters, 1302
  - Collect\_Message\_Tracking\_Log\_Statistics script parameters, 1303
  - Collect\_Public\_Folder\_Statistics script parameters, 1302-1303
  - VerifyEAS script parameters, 1301
  - VerifyMAPI script parameters, 1301
  - VerifyMFR script parameters, 1300
  - VerifyOMA script parameters, 1301
  - VerifyOWA script parameters, 1301
- Exchange Server 2003 management pack, tuning, 723-724
- explained, 111-114, 593-594
- exporting, 634-635
- extensible monitoring, 598
- FRS, 512
- forwarding alerts by email, 690
- hardware management packs, importing, 865-872, 874-877
- HP Server Management Packs for OpsMgr 2007, 1114-1116
- IBM Director Management Pack, 1118
- identifiers, 1165
- IIS management pack, 1254-1255
- importing, 636-640
  - during installation, 594
  - with Operations console, 636-638
  - with PowerShell, 638
  - verifying installation, 639-640
- on installation media, 332
- integration, 323
  - default management packs, 323-325
  - importing management packs, 326-332
  - selecting management packs, 326
- knowledge in, 598-599
- listing, 641-642
- maintenance, 195
- migration, 289
- model-based management, 594
- MOM 2005 management packs, converting, 619-621
- monitoring clients, 830-842
- MP2XMLDumper utility, 644-645
- objects, explained, 600
- OLE DB, 922-928
- online information, 615-616
- Operations Manager Automatic Agent Management Library, 640
- Override Explorer, 642

- overrides, 597, 706
  - best practices, 715
  - creating, 707-712
  - defining, 706-707
  - finding, 712-715
  - naming, 612
- overview, 1141-1142
- packaging RDL files in, 583
- proxying agents, 407
- ReSearch This! management pack, 1308
- resultant set of rules, viewing, 642-644
- Run As Accounts, 489
- sample management pack
  - configuring, 1220-1224
  - creating, 1217-1220
  - installing, 1220-1224
  - overview, 1216
  - sealing, 1223-1224
- schema file for, 595
- sealed management packs, 117, 596
  - creating, 614-615
  - updating, 596
  - viewing, 634-635
- SQL Server management pack
  - installation, 1249-1250
  - object discovery, 1250-1251
  - tuning and alerts, 726-727, 1251-1253
- structure of, 595-599
- System Center Internal Task Library MP, 640-641
- System Center Pack Catalog, 1164
- tasks in, 601-602
- test environments, 631
- troubleshooting, 630-634
- uninstalling, 598
- Unisys ES7000 Management Pack, 1118
- unsealed management packs, 596
- updates, 90, 616
- verifying with MPVerify utility, 615
- versions of, determining, 617-619
- viewing, 641
- Virtual Machine Manager management pack, 1043
- VMWare management packs, 1034

- Web Application Management Pack Template, 1256-1258
- Windows Server Operating System management pack, tuning, 726
- workflows, 602
  - diagnostics, 604
  - discoveries, 603-604
  - monitors, 604
  - recoveries, 605
  - rules, 602-603
  - tasks, 604
- XML documents
  - management pack creation, 1170-1175
  - overview, 1161-1162
  - sample management pack XML file, 1165-1170
  - viewing in Internet Explorer, 1166
  - viewing in XML Notepad, 1166, 1168
- XML management pack structure, 1163-1164
- Management Server Action account, 165, 493**
- Management Server Component, 224**
- Management Server Computer Group, overrides, 626**
- management servers, 103**
  - configurations, 425
  - multihomed deployments, 431-433
  - multilocation deployments, 426-429
  - multiple management groups, 430-431
- in Device Management node, 357
- failover for gateway servers, 436
- hardware requirements, 151-152
- Health service on, 106
- load balancing and redundancy, 426-427
- network bandwidth utilization, 145
- online information, 1306
- operating system requirements, 157
- performance counters, 1264-1267
- placement in multiple-server configuration example, 175-176
- promoting to RMS, 589
- Registry keys, 1276-1279
- restoring RMS to, 572-576
- sizing and capacity limitations, 180-181

- ManagementPack table, 619
- ManagementServerConfigTool, 464-465
- Manifest section (management pack schema), 118, 1163
- manual agent installation, 402-403, 412-413
- manually resetting monitors, 686-687
- manually setting Local Security Policy, 743
- MAPI, monitoring logons, 939
- markup languages, 1161
- Master database, backing up, 541
- Master Hoster ROM, 1060-1062
  - Audit Collection Services, 1063
  - customers-per-gateway capacity, 1063-1065
  - redundant configurations, 1063
- MaximumQueueLength value (ACS collector performance), 774
- McAllyn, Duncan, 1215
- MCF (MOM Connector Framework), 1107
- MDOP (Microsoft Desktop Optimization Pack), 800
- memory leaks from timed scripts, 620
- memory performance, 468-469
- Memory Pool Non-Paged Bytes Monitor, 967
- messages (SNMP), 846-848
- messaging, capturing Syslog messages, 1135-1137
- Messaging templates, 994-996
- methodology, lack of, 18, 51
- methods (authentication), configuring, 919
- MIB walkers, 878
- MIB-2 OIDs, populating, 852
- MIBs (Management Information Base), 848-850, 878-880
- Microsoft, 247
  - acquisition of Engyro, 1109
  - acquisition of NetIQ, 65
  - error reports, sending to, 247
  - management strategy, 22
    - DSI, 22-25
    - IO Model, 31-34
    - ISO 20000, 31
    - ITIL, 26-31
    - MOF, 26-31
    - online information from, 1310-1313
- Microsoft Core XML Services (MSXML), 266
- Microsoft Desktop Optimization Pack (MDOP), 800
- Microsoft Excel, viewing CSV files, 713
- Microsoft Exchange
  - importing, 938
  - monitoring, 933-935, 939-940
- Microsoft Forefront, security, 1140
- Microsoft Generic Report Library, 375
- Microsoft Internet Security and Acceleration (ISA) Server, 1070-1071
- Microsoft ODR Report Library, 376
- Microsoft Operations Framework. *See* MOF
- Microsoft Operations Manager. *See* MOM
- Microsoft Privacy Statements, CEIP and, 823-828
- Microsoft Solutions Framework (MSF), 28, 138
- Microsoft System Center, 54
- Microsoft System Center Desktop Error Monitoring (DEM), 800
- Microsoft Systems Management Server, 393
- Microsoft Volume License (MVLS) website, 279
- Microsoft Word, 700
- Microsoft.interop.security.azure.dll, 250
- middleware, 950
- migration
  - case studies, 288-298
  - documentation, 280
  - new hardware, 284-288, 297-298
  - planning, 277-278
  - same hardware, 281-296
  - security, management packs, 289
  - starting clean, 278-281
  - summarizing, 295-296
  - troubleshooting, 299-300
- Migration Tool, running, 289-290, 292
- minimum security log settings, 745
- Mission Critical Software, 65
- Mobile console, 360
- model-based management, 71, 594

**models, 71, 110, 115, 594**

- health models, explained, 115-117
- report models
  - creating, 1203, 1206
  - deploying, 1206
- service modeling, explained, 111-115

**modification**

- agents
  - configuring settings, 414
  - manual installation, 412-413
  - state, 408
- approval processes, 373-374

**module types, 126-127, 607-608**

**modules**

- data types, 605
- in rules, 602

**MOF (Microsoft Operations Framework), 26-31, 138**

- explained, 28-30
- ITIL relationship with, 31
- online information, 1312

**MOM (Microsoft Operations Manager), 204, 277**

- agents, coexisting with, 409
- management packs for, 617
- migration
  - case studies, 288-298
  - new hardware, 284-288, 297-298
  - planning, 277-278
  - same hardware, 281-283, 288-296
  - starting clean, 278-281
  - troubleshooting, 299-300

**MOM 2000 Service Pack (SP) 1, 64**

**MOM 2005**

- capacity changes in OpsMgr 2007, 91-92
- environments in assessment
  - documents, 139
- functionality changes in OpsMgr 2007, 71-88
- management packs
  - changes in OpsMgr 2007, 89-90
  - converting, 619-621
- reporting changes in OpsMgr 2007, 88-89
- summary of changes in OpsMgr 2007, 90-91

- system requirements, 92-93
- targeting rules, 595
- terminology changes in OpsMgr 2007, 69-71

**MOM 2005 Backward Compatibility, 376**

**MOM 2005 Service Pack (SP) 1, 65**

**MOM 2005 SharePoint WebPart, troubleshooting, 1030**

**MOM Connector Framework (MCF), 1107, 1288**

**MOMAuth.xml files, editing, 484**

**MOMCertImport tool, 513, 517-519**

**MOMInventory tool, 590-591**

**MOMNetCheck utility, 1307**

**monitor overrides, 609**

**Monitor Wizard, services in, 676**

**monitored computers, 1261**

**monitored servers, design stage (deployment planning), 164**

**monitoring. *See also* monitors**

- AEM, 211, 418
  - clients, 805-814, 816-819
  - installation, 268-269, 271
  - reporting, 819-823
- agentless, deployment, 404-405
- agents, 208
  - defining failover, 414, 416
  - deleting, 417-418
  - disk performance, 412
  - event logs, 410-412
  - pending actions, 412-414
  - queue files, 416-417
- alerts, 648, 687-688
  - generating, 688-690
  - knowledge, adding, 699-703
  - notification workflow, 691, 693-699
  - tuning, 718-719, 723-727
  - views, creating, 720-723
- business critical, 804, 829, 838-843
- clients
  - agent-managed systems, 828-842
  - CEIP and Microsoft Privacy Statements, 823-828
  - CER, 799-800
  - cost of end-user problems, 802-803

- features, 797-798
- machines, 800-802
- new features, 803-805
- operating systems, 379
- synthetic transaction monitoring, 843
- Windows Error Reporting, 798-799
- Collective Client Monitoring, 832-837
- crashes, 807, 809-812
- customer network devices with ROM, 1073
- disabling with maintenance mode, 727-730
- distributed applications, 1039
- email flow, 939
- ESX monitoring, 1130
- extensible monitoring, 598
- external sites, 999
- hangs, 807, 809-812
- importance of, 648-649
- MAPI logons, 939
- monitors, 648, 667-668
  - finding in Operations console, 703-706
  - log file monitor, 679-680
  - manually resetting, 686-687
  - SNMP monitor, 679-680
  - Windows Events monitor, 668, 681-686
  - Windows Performance Counters monitor, 668-675
  - Windows service monitor, 675-678
  - WMI event and performance monitors, 680
- network devices, 384, 845
- networks, 801
- objects, distributed applications, 992
- original solutions, decommissioning, 280
- overrides, 706
  - best practices, 715
  - creating, 707-712
  - defining, 706-707
  - finding, 712-715
- proactive monitoring, 1006
- processes, 679
- resolution states, creating custom, 716-718
- RMS clustered nodes, 223
- rules, 648-649
  - alert-generating rules, 649-653
  - collection rules, 653-662
  - creating, 649
  - finding in Operations console, 703-706
  - timed commands, 663-665
- security, 471, 480
- SSL monitoring, troubleshooting, 1258
- state monitors, alerts versus, 719
- synthetic transaction, 804, 829, 843
  - applications, 940-941, 944, 947
  - databases, 922-923, 925-928
  - Exchange, 933-935, 939-940
  - ports, 928, 930, 932-933
  - predicting behavior by simulation, 905
  - watcher nodes, 906-907
  - Web applications, 907-909, 912-920
- TCP ports, 1131-1135
- with Web Application Management Pack Template, 1256-1258
- Web Console Component, 228
- monitoring engine, 83-85**
- Monitoring Overview page (Operations console), 307-308**
- Monitoring pane (Operations console), 131, 344-351**
- Monitoring section (management pack schema), 119, 1163**
- monitoring solutions in assessment documents, 139**
- monitoring tools**
  - history of, 64-65
  - OpsMgr 2007, as centralized monitoring, 37-39
  - wealth of information available, 35-36
- MonitoringHost.exe process, 492**
- monitors, 70, 84, 119, 354-355, 604, 648, 667-668. See also monitoring**
  - AD\_Client\_Connectivity script parameters, 1299
  - AD\_Client\_GC\_Availability script parameters, 1300
  - AD\_Client\_PDC\_Response script parameters, 1300

- AD\_Database\_and\_Log script parameters, 1296-1297
- AD\_Essential\_Services\_Running script parameters, 1299
- AD\_General\_Response script parameters, 1297
- AD\_Global\_Catalog\_Search\_Response script parameters, 1297
- AD\_Op\_Master\_Response script parameters, 1298-1299
- AD\_Replication\_Monitoring script parameters, 1296
- aggregate monitors, 117, 120-121
- Collect\_Mailbox\_Statistics script parameters, 1302
- Collect\_Message\_Tracking\_Log\_Statistics script parameters, 1303
- Collect\_Public\_Folder\_Statistics script parameters, 1302-1303
- creating with Operations console, 1143-1149
- custom SNMP monitors, 877-878
  - creating, 894-901
  - SNMPUTIL.exe utility, 878-880
- data sources for, 85
- dependency monitors, 121-122
- disabling, 623, 629
- explained, 120-121
- finding in Operations console, 703-706
- front-end monitors, configuring (Exchange Services), 970
- in health model, 115-117, 120
- log file monitor, 679-680
- manually resetting, 686-687
- overrides, 629
- rules versus, 84, 897
- SNMP monitor, 679-680
- state icons, 120
- targeting, 123, 665-666
- thresholds, changing, 629
- types of, 604
- unit monitors, 123-126, 1182
- VerifyEAS script parameters, 1301
- VerifyMAPI script parameters, 1301

- VerifyMFR script parameters, 1300
- VerifyOMA script parameters, 1301
- VerifyOWA script parameters, 1301
- viewing AD health, 959-961
- Windows Events monitor, 668, 681-686
- Windows Performance Counters monitor, 668-675
- Windows service monitor, 675-678
- WMI event and performance monitors, 680

## **moving**

- ACS database, 569-570
- Data Warehouse database, 567-569
- Operations database, 565-567

## **.MP file extension, 1164**

**MP Notifier management pack, 616**

**MP Studio (Silect), 1183-1188**

**MP2XML utility, 620**

**MP2XMLDumper utility, 644-645**

**MPConvert utility, 620**

**MPSeal utility, 614-615**

**MPVerify utility, 615**

**MPViewer utility, 641**

**MsdB database, backing up, 541**

**MSF (Microsoft Solutions Framework), 28, 138, 1312**

**MSPs (Managed Service Providers), 966**

**MSXML (Microsoft Core XML Services), 266**

**multihomed agents, 99, 409-410, 432**

**multihomed deployments, 214, 431-433**

**multihomed management groups, 147-148**

**multilocation deployments, 426, 428-429**

**multiple domains, planning, 216, 218**

**multiple management groups, 104, 176-177, 188-189, 430-431**

**multiple management servers, load balancing and redundancy, 426-427**

**multiple MonitoringHost.exe instances, 493**

**multiple-management group design sample, 198, 200**

**multiple-server configuration example, 174-178**

**multiple-server Operations Manager installation, 241**

**mutual authentication, 217, 503-507, 511**

**MVLS (Microsoft Volume License) website, 279**  
**My Views, creating, 366**  
**My Workspace pane (Operations console), 131, 366-367**

## N

**name resolution, 1079**  
**named instances (SQL Server), ACS connections, 751**  
**names (discovery process), troubleshooting, 372**  
**naming**  
     agents, 417-418  
     backups, 556  
     data warehouse server, location of name, 569  
     databases, 80-81  
     management groups, 100, 144  
     management packs for overrides, 612  
     UNC, 799  
**NAP (Network Access Protection), 55**  
**navigation button area (Operations console), converting to toolbar, 132**  
**navigation panes in Operations console**  
     Administration space, 357-362  
     Authoring space, 352-357  
     list of, 343-344  
     Monitoring space, 344-351  
     My Workspace space, 366-367  
     Reporting space, 362-365  
**NetIQ, Microsoft acquisition of, 65**  
**Network Access Protection (NAP), 55**  
**network bandwidth utilization, 145**  
     agents, 179  
     multiple-server configuration example, 175  
     online information, 1307  
**network connectivity requirements, 144**  
**Network Device Library, 376**  
**Network Device Monitoring Library, 865-871**

**network devices, 850**  
     in Device Management node, 357  
     discovering, 850-864  
         adding with Discovery Wizard, 853-856  
         adding with PowerShell, 857-859  
         changing proxy agents, 859-863  
         preparations for, 850-852  
         SNMP polling conversation contents, 864  
     hardware management packs, importing, 865-877  
     MIBs, examining, 878-880  
     monitoring, 845  
     OIDs, discovering, 878-880  
     performance reports, creating, 892-894  
     populating contact and location fields, 868  
     SNMP support, 877  
**network elements, 846**  
**network environment, management group design, 144**  
**network management, 1048**  
     smaller-sized organizations, 1048-1049  
     SMB service providers, 1050-1052  
     tools for measuring service, 1049-1050  
**Network Management System (NMS), 846**  
**Network Operations Centers, 1050**  
**network performance, 470**  
**network traffic, reducing, 429-430**  
**networks**  
     customer networks, 1082  
     devices, 384  
     monitoring, 801  
**new hardware migrations, 284-288, 297-298**  
**newsgroups, list of, 1321-1322**  
**NMS (Network Management System), 846**  
**NOCs (Network Operations Centers), 1050**  
**nodes, 223, 441**  
**non-domain controllers, minimum security log settings, 745**  
**non-trusted domains (OpsMgr), 504, 506**  
**non-Windows systems, managing**  
     eXc software, 1121-1123  
     Jalasoft Xian IO, 1123-1127  
     networks VMware Management, 1128-1130



overview, 1120-1121

Quest Management Xtensions, 1128

Syslog message capturing, 1135-1137

TCP port monitoring, 1131-1135

**Notepad, changing log file location with, 322**

**Notification Action account, 165, 488, 499**

**notification channels, 1015**

**notification of problems, lack of, 16-17, 40-43**

**notification workflow, 689-699**

recipients, creating, 693-695

subscriptions, creating, 695-699

**notifications, 83, 648, 1015-1016, 1092, 1119-1120**

configuring, 689-690

design stage (deployment planning), 165

online information, 1309

print spooler alerts, 1164

**Notifications Internal Library, 376**

**Notifications node (Administration space), 361**

**notifications settings, 358**

**NotMyFault.exe, 810**

**nworks VMware Management, 1128-1130**

## O

**Object Access report, 788**

**object discoveries, 355**

rules, 114-115

SQL Server management pack, 1250-1251

**Object Identifiers, 848**

**Object Linking and Embedding Database, 922**

**Object override, 610**

**Object Picker, Line of Business Web application templates, 990-992**

**object-oriented reporting, 89**

**objects, 51**

adding, 944

classes and, 601

creating, 354-357

describing, 112-113

discovering, 333-335

explained, 600

GPO, event log configuration, 412

relationships between, 112-114

**ODBC data source, viewing, 752**

**ODBC Data Source Administrator, 752**

**ODRs (Operational Data Reports), 824**

**OGC (Office of Government Commerce), 26**

**OIDs (Object Identifiers), 848-850, 878-880**

**OLE DB (Object Linking and Embedding Database), monitoring, 922-923, 925-928**

**OLE DB Data Source template, 352**

**OLE DB Data Sources, creating, 980-981**

**OM 2007. See OpsMgr 2007**

**OMCF (Operations Manager Connector Framework), 1107**

**OML (Operations Management License), 159-162, 999**

**on-demand detection (monitors), 604**

**on-demand diagnostic tasks, 1008**

**online information**

ACS, 1305-1306

architecture, 1307

blogs, 1314-1316

Certificate Services, 1306

client monitoring, 1306

Command Shell, 1316

connectors, 1318-1321

deleting agentless systems, 1309

diagnostics and recoveries, 1009

Exchange Server Management Pack Configuration Wizard, 1313

Gateway Server, 1306

IO Model, 1312

maintenance mode, 1309

management packs, 615-616

management servers, 1306

MOF, 1312

MSF, 1312

network bandwidth utilization, 1307

notifications, 1309

OpsMgr 2007, 1305-1313

PowerShell, 1316-1317

property bags, 1310

- public newsgroups, 1321-1322
- Remote Operations Manager, 1318
- ReSearch This! management pack, 1308
- Resource Kits, 1313
- Service Manager, 1318
- SharePoint Monitoring Toolkit for OpsMgr, 1312
- SRS Recovery Planning, 1308
- System Center components, 1317-1318
- System Center Essentials, 1317-1318
- System Center Pack Catalog, 1310
- System Center Roadmap, 1317
- training courses, 1307
- training videos, 1312
- virtual machines, 1309
- virtual server clusters, 1308
- Visual Studio 2005 Tools for Office Second Edition Runtime, 1313
- XML Notepad 2007, 1312
- OOMADS (Active Directory Helper Object), 285**
- OpenManage, 871**
- OpenView, 871**
- Operating quadrant (MOF), 30**
- Operating System Deployment (OSD), 55, 395**
- operating systems**
  - clients, monitoring, 379
  - requirements, server components, 156-159
- Operational Data Reports (ODRs), 824**
- Operations console, 73, 130-132, 203, 228**
  - ACS administration, 767-769
  - adding network devices, 853-856
  - Administration space, 357-362
  - Authoring space, 352-357
  - backing up management packs, 580-582
  - configuration data, 342
  - connections, 338-339
  - console errors, 339-341
  - editing company knowledge, 339
  - favorite reports, 1190-1193
  - finding rules/monitors in, 703-706
  - hardware requirements, 155
  - importing management packs, 326-329, 636-638
  - installation, 305-307
    - with Configuration Manager, 1023
  - requirements, 336-337
  - management packs, creating, 1142
  - Monitoring space, 344-351
  - My Workspace space, 366-367
  - navigation panes, list of, 343-344
  - Registry keys, 1291-1292
  - Reporting space, 362-365
  - Scope feature, 623
  - scoping, 704-706
  - search feature for network devices, 868
  - uninstalling management packs, 598
  - where to run, 305, 335-336
  - without trusted authentication, 340-342
- Operations database, 100**
  - availability of, 108
  - backing up, 540, 554
    - importance of, 464
    - steps in, 554-560
  - truncating transaction log, 560, 562-563
  - determining size of, 632
  - grooming, 545
  - hardware requirements, 152-154
  - ManagementPack table, 619
  - moving, 565-567
  - multiple-server configuration example, 177-178
  - recovery mode, changing, 448
  - restoring, 564-565
  - security, 502-503
  - sizing and capacity limitations, 181-184
- Operations database clusters, installing, 447-448**
- Operations Database Component, 225-226**
- Operations Database Server, 203, 242-243, 245-248**
- operations management, defined, 20-22**
- Operations Management License (OML), 159-162, 999**
- operations management problems, 13-14, 19**
  - expertise, lack of, 18, 48-50
  - false alarms, 19, 52-54
  - historical information, lack of, 17, 44-49

- islands of information, 15-16, 37-39
- methodology, lack of, 18, 51
- missing information, 18-19, 51
- notification, lack of, 16-17, 40-43
- security policy enforcement, 43-44
- system outages, reasons for, 14-15
- wealth of information, 35-36

**Operations Manager. See OpsMgr 2007**

**Operations Manager Agent Management Library, 376**

**Operations Manager Agents, 204**

**Operations Manager Automatic Agent Management Library, 640**

**Operations Manager Connector Framework (OMCF), 1107**

**Operations Manager Event log, 317**

**Operations Manager Internal Library, 376**

**Operations Manager Inventory, 590-591**

**Operations Manager Management Group, 954-955**

- Alerts view, 955-956
- Diagram view, 956, 958
- Performance view, 955-956

**Operator role, 78**

**OpsMgr 2007**

- Active Directory integration, 1033-1034
- architectural overview, 98
  - management groups, 98-100
  - server components, 100-105
- agents, 229
- Authoring console
  - classes, 1178, 1180-1181
  - overview, 1175-1177
  - unit monitors, 1182
- benefits of, 36-37
- blogs about, 1314-1316
- branding for, 67-68
- capacity changes, 91-92
- Capacity Planner integration, 1024-1025
- as centralized monitoring system, 37-39
- communication protocols, 108-110
- compared to alternate enterprise monitoring solutions, 1097
- components, 213, 949

Configuration Manager integration, 1022-1024

connected management groups

- advantages, 1100
- establishing connections, 1101-1105
- example, 1099-1100
- overview, 1096-1097
- prerequisite tasks, 1103-1105
- security, 1100
- viewing connected data, 1106

connections, planning, 219-221

deleting, 271-272

Deployment Guide, 1107

deployment planning, 137

disaster recovery, 586

as distributed application, 1038

DSI integration, 23

evaluation copy, 92

Exchange 2007 integration, 1031-1033

expertise, built-in, 48-50

false alarms, reducing, 52-54

focus of, 67-68

functionality changes, 71-88

- ACS, 86

- Active Directory integration, 79-80

- Agentless Exception Monitoring, 72

- agents, 83

- client monitoring, 85

- Command Shell, 76

- connected management groups, 85

- connector framework, 85

- consoles, 73-75

- data flow, 86-88

- database clustering, 82-83

- database naming, 80-81

- Health Explorer, 75-76

- maintenance mode, 83

- model-based management, 71

- monitoring engine, 83-85

- notifications, 83

- Registry keys, 81

- role-based security, 77-78

- Run As Accounts, 79

- Run As Profiles, 78
- self-tuning thresholds, 83
- server components, 81-82
- service-oriented monitoring, 71-72
- services, 79
- SNMPv2 support, 76
- WS-Management support, 76
- health models, explained, 115-117
- historical information, viewing, 44-49
- history of, 64-65
- integrating with other system center applications, 1138-1139
- management groups, installing System Center Essentials on customer networks, 1075-1076
- management pack schema, explained, 117-119
- management packs, 1114
  - changes in, 89-90
  - Citrix Presentation Server Management Pack, 1118-1119
  - Dell Server Management Pack, 1116
  - HP Server Management Packs for OpsMgr 2007, 1114-1116
  - IBM Director Management Pack, 1118
  - Unisys ES7000 Management Pack, 1118
- methodology in, 51
- missing information, catching, 51
- MOF support, 30
- monitors
  - aggregate monitors, 120-121
  - dependency monitors, 121-122
  - explained, 120-121
  - unit monitors, 123-126
- multiple-server configuration example, 174-178
- non-trusted domains, 504, 506
- non-Windows systems, managing
  - eXc software, 1121-1122
  - Jalasoft Xian IO, 1123-1127
  - nworks VMware Management, 1128-1130
  - overview, 1120-1121
  - Quest Management Xtensions, 1128

- Syslog message capturing, 1135-1137
- TCP port monitoring, 1131-1135
- notifications, 40-43, 1119-1120
- online information, 1305-1313
- PowerShell integration, 1026-1029
- preparing for ROM, 1065
  - Active Directory, 1065-1067
  - Certificate Authority, 1067-1070
  - DMZ, 1070
  - DNS, 1065-1067
  - firewalls, 1070-1072
  - installing Service Provider management pack, 1072-1073
- presentation layer, 129-130
  - Operations console, 130-132
  - PowerShell, 132-134
  - Web console, 132
- product connectors
  - HP-OVO connections, 1109-1110
  - overview, 1107-1109
  - third-party connectors, 1112-1114
  - Tivoli TEC connections, 1110, 1112
- reasons for using, 12-13
- Registry keys, 1273-1274
  - ACS forwarder, 1286-1287
  - ACS server, 1284-1286
  - agents, 1274-1276
  - certificates, 1293
  - Configuration service, 1280-1281
  - current logged-on user, 1291-1292
  - Data Warehouse server, 1281
  - database server, 1281
  - event log, 1287-1288
  - Health Service, 1288-1291
  - management servers, 1276-1279
  - MOM Connector, 1288
  - PowerShell, 1282-1283
  - report server, 1282
  - SDK service, 1279-1280
- reports, 54
  - backing up, 583
  - changes to, 88-89
- scalability of, 52

security policy enforcement, 43-44  
 Service Manager integration, 1029  
 service modeling, explained, 111-115  
 SharePoint integration, 1029, 1031  
 single-server configuration example, 169-171  
 state-based management, explained, 117  
 summary of changes, 90-91  
 System Center Essentials versus, 94-95  
 system requirements, 92-93  
 targeting rules, 595  
 terminology changes, 69-71  
 transitioning to ROM, 1052  
 two-server configuration example, 170-174  
 value of, 59-61  
 Virtual Machine Manager integration, 1025-1026  
 VMWare integration, 1034  
 Windows services, 104  
     Audit Collection service, 108  
     Audit Forwarding service, 107  
     Config service, 107  
     Health service, 105-106  
     SDK service, 106-107  
 workflows  
     cook down, 128-129  
     data types, 129  
     explained, 126-129  
     module types, 126-127  
 workgroups, 506-507, 511

#### **OpsMgr 2007 Service Pack 1, 66-67, 574**

**OpsMgr Config Service per Agent performance counters, 1265**

**OpsMgr Config Service performance counters, 1265**

**OpsMgr Connector performance counters, 1267-1268**

**OpsMgr DB Write Action Cache performance counters, 1266**

**OpsMgr Distributed Application (DA), 952-953**

**OpsMgr DW Synchronization Module performance counters, 1266**

**OpsMgr DW Writer Module performance counters, 1267**

**OpsMgr SDK Service performance counters, 1265**

**OpsMgr Web console performance counters, 1269**

**OpsMgr Write Action Modules performance counters, 1266**

#### **optimization**

agents, 412

IO Model, 31

**optimized collections, 655-657**

**Optimizing quadrant (MOF), 30**

#### **options**

Action accounts, 494

migration, 278

web addresses, 917

**order of implementation for management packs, 621-622**

**order of installation, 240**

**OSD (Operating System Deployment), 55, 395**

**OU (Organizational Unit), 371, 1066**

**"OutOfMemoryException" error message, 638**

**output (reports), creating, 1214-1215**

**Override Explorer, 642, 1309**

**overrides, 119, 608-611, 706**

best practices, 715

creating, 707-712

defining, 706-707

finding, 712-715

management packs, 597

Management Server Computer Group, 626

of monitors/rules, 356, 629

storage location for, 611-612

types of, 610

viewing, 610

**Overrides Explorer, 714-715**

**overwriting backups, 556**

**OWA certificate, piggybacking, 1082**

**OWA logon failure, troubleshooting, 1244-1246**

## P

**p\_partitioningandgrooming stored procedure, 545**

**packaging RDL files in management packs, 583**

**packs. See management packs**

**parameters**

- AddReportingUserRole.ps1, 482
- AD\_Client\_Connectivity script, 1299
- AD\_Client\_GC\_Availability script, 1300
- AD\_Client\_PDC\_Response script, 1300
- AD\_Database\_and\_Log script, 1296-1297
- AD\_Essential\_Services\_Running script, 1299
- AD\_General\_Response script, 1297
- AD\_Global\_Catalog\_Search\_Response script, 1297
- AD\_Op\_Master\_Response script, 1298-1299
- AD\_Replication\_Monitoring script, 1296
- Collect\_Mailbox\_Statistics script, 1302
- Collect\_Message\_Tracking\_Log\_Statistics script, 1303
- Collect\_Public\_Folder\_Statistics script, 1302-1303
- for reports, 363-364, 614
- overriding, 712
- VerifyEAS script, 1301
- VerifyMAPI script, 1301
- VerifyMFR script, 1300
- VerifyOMA script, 1301
- VerifyOWA script, 1301

**partner contacts, notifications, 1092**

**Password Change Attempts by Non-Owner report, 786**

**passwords (Action accounts), modifying, 496**

**patch management, 1036-1037**

**paths (UNC), 799**

**pending actions, agent management, 412-413**

**pending management in Device Management node, 357**

**performance. See also performance counters**

- alert latency, 153
- disk performance, 469-470
- disks, agent management, 412
- memory performance, 468-469
- network performance, 470
- OLE DB, viewing, 928
- processor performance, 156, 470
- TCP ports, viewing, 932-933
- websites, viewing, 920

**performance collection rules, 70**

- creating, 654-656
- optimized collections, 655-657

**performance counters, 16**

- maintained by ACS Collector, 1269-1270
- maintained by agents, 1261-1264
- maintained by management servers, 1264-1267
- maintained by OpsMgr Connector, 1267-1268
- maintained by OpsMgr Web console, 1269
- tuning, 180
- Windows Performance Counters monitor, 668-675
- for websites, 908
- viewing, 920

**performance health monitors, 121**

**Performance Library, 376**

**performance management for ACS collectors, 773, 775-777**

**Performance Monitor, ACS counters, 777**

**performance reports for network devices, creating, 892-894**

**Performance view**

- for distributed applications, 314-315
- Operations Manager Management Group, 955-956

**performance-based collection rules, 880, 890, 892-894**

**permissions**

- Action accounts, 494
- for Gateway Approval Tool, 436
- granting on ACS database, 754-755
- migration, management packs, 289
- role-based security, 480

**permitted SNMP managers, enabling, 851**

**permitting ACS drivers, 395**

**Personalize view, 345-346**

**personalizing Computers global view, 345-346**

**phased deployment, 194**

**physical locations, management group  
design, 143**

**piggybacking OWA certificate, 1082**

**pilot stage (deployment planning), 191-194**

**pivoting views, 311**

**PKI (Public Key Infrastructure), 1056**

**planning**

Active Directory integration, 218-219

audit policies, 741-746

components, 203

ACS, 206-208

AEM, 211

Gateway Server Component, 208

managing agents, 208

reporting/trending, 204-206

Web Console Server, 212

connected management group  
deployments, 215

highly available configurations, 221-229

installation, 234

migration, 277-278

multihomed deployments, 214

multiple domains, 216, 218

Operations Manager connections, 219-221

Operations Manager deployment, 137

**Planning category (audit reports), 783**

**POC. See proof of concept**

**policies**

AEM, deploying, 807, 809-812

audit policies, 740

Group Policy deployment, 391-392

security policies, 741

**policy changes scenario (audit reports),  
789-794**

**populating**

dynamic computer groups with Health  
Service watchers, 1018

MIB-2 OIDs, 852

network device contact and location  
fields, 868

**ports**

default ports, list of, 108-110

firewalls, 530-532

monitoring, 928, 930, 932-933

TCP port monitoring, 1131-1135

tools, 420

**PowerGUI, 1027**

**PowerShell, 73, 132-134, 578**

for Active Directory, 1027

adding network devices, 857-859

agent installation, 403-404

backing up management packs, 577-580

computer discovery, scheduling, 372-373

email-enabled user accounts,  
creating, 1032

enabling ACS, 763

help information, 1028

importing management packs,  
329-330, 638

integration for distributed applications,  
313-314

integration with, 1026-1027, 1029

listing management packs, 641-642

online information, 1316-1317

Registry keys, 1282-1283

**predefined distributed applications, 958**

**predefined Registry keys, 1271-1272**

**predicting behavior by simulation, 905**

**preparations for network device discovery,  
850-852**

**prerequisites. See requirements**

**presentation layer of OpsMgr 2007, 129-130**

Operations console, 130-132

PowerShell, 132-134

Web console, 132

**Presentation section (management pack  
schema), 1164**

**Presentation Server Management Pack (Citrix),  
1118-1119**

**presentation types, 612-613**

**PresentationTypes section (management pack  
schema), 1164**

**printing print spooler alerts, 1164**

**privacy, Microsoft Privacy Statements, 823-828**

**Privileged Monitoring profile, 488**

**proactive monitoring, 1006**

**probe action module type, 127-128, 608**

**probe-based detection monitors (SNMP), creating, 895-898**

**probe-based rules, 657**

**probes, 653**

**processes**

- monitoring, 679
- MonitoringHost.exe process, 492

**processing power requirements, management group design, 146**

**processor performance, 156, 470**

**product connectors, 362**

- HP-OVO connections, 1109-1110
- overview, 1107-1109
- third-party connectors, 1112-1114
- Tivoli TEC connections, 1110, 1112

**product knowledge, viewing, 49-50**

**production environments, test environments versus, 143**

**products, connectors, 219-220**

**profiles, 143, 474**

- management servers, adding to run as, 503
- Run As Profiles, 487-488

**promoting management servers to RMS, 589**

**proof of concept (POC)**

- in deployment planning, 190-193
- environment, 277
- exclusion, 192

**properties, 51**

- domains (Windows), 236
- web applications, configuring, 914
- of Windows Computer group type, 1017

**property bags**

- definition, 1220
- online information, 1310

**protocols**

- communication protocols, list of, 108-110
- TCP, port monitoring, 1131-1135

**providers, 647**

- for alert-generating rules, 649
- Windows SNMP trap provider, 680

**provisioning**

- applications, 1039-1040
- servers, 1042-1045
- user accounts, 1040-1041

**proxy agents for network devices, changing, 859-863**

**proxying agents, 405-408, 511-512**

**Public Key Infrastructure, 1056**

**public newsgroups, list of, 1321-1322**

**publishing reports, 1193, 1195-1197**

**publishing rules (firewalls), 1071-1072**

## Q-R

**queries**

- OLE DB synthetic transactions, 925-927
- ports, utilities, 420

**Quest Management Xtensions, 1128**

**queue files, 565**

**queue size, 633**

**queues, 416-417**

**quorum, 441**

**RAID arrays, disk performance, 469-470**

**RAS deployment approach (Ready, Aim, Shoot), 137**

**Rationalized level (IO Model), 34**

**RDL files, packaging in management packs, 583**

**read-only management packs, 596**

**Read-Only Operator role, 78**

**recipients of notifications, 361, 689, 693-695**

**recording (SSL), 909**

**recoveries, 119, 554, 605**

**recovery mode for Operations database, changing, 448**

**recovery tasks, 1008-1010**

- console tasks and, 1019-1021
- creating, 1013-1014
- restarting Health service, 1014

**reducing network traffic, 429-430**



**redundancy, 437, 439-440**

- ACS collector, 452
- clusters, 440-441
  - ACS clusters, installing, 451-452
  - AEM clusters, installing, 454
  - complex database clusters, installing, 452-454
  - data warehouse clusters, installing, 449-451
  - installing, 441-442
  - Operations database clusters, installing, 447-448
  - reporting server clusters, installing, 455-457
  - RMS clusters, installing, 457-467
  - SQL Server 2005 clusters, installing, 443-447
  - testing failover, 442-443
- for gateway servers, 436-437
- log shipping, 448-449
- of management servers, 151
- with multiple management servers, 426-427
- multiple-server configuration example, 176
- options for, 438-439
- of Web Console Server, 458

**reference element (management packs), 1168**

**reference URLs, 1305**

**refresh interval for Web console, 366**

**regedit.exe utility, 1271**

**registration,**

**Microsoft.interop.security.azure.dll, 250**

**Registry, 1271**

- disabling version checking in, 66
- explained, 1271-1273
- hives, 1272
- keys
  - AeDebug, applying, 811
  - changes to, 81
  - predefined, 1271-1272
- OpsMgr-related keys, 1273-1274
  - ACS forwarder, 1286-1287
  - ACS server, 1284-1286
  - agents, 1274-1276

    certificates, 1293

    Configuration service, 1280-1281

    current logged-on user, 1291-1292

    Data Warehouse server, 1281

    database server, 1281

    event log, 1287-1288

    Health Service, 1288-1291

    management servers, 1276-1279

    MOM Connector, 1288

    PowerShell, 1282-1283

    report server, 1282

    SDK service, 1279-1280

**Registry Editor, 1271**

**relationship discovery rules, 114-115**

**relationship types, 607**

**relationships, 51, 112-114**

**release cycles (distributed applications), 950, 952**

**remote agents, prerequisites, 385**

**Remote Operations Manager. See ROM**

**remote watcher nodes, 906**

**Remote Web Workplace (RWW), 1058-1060, 1080-1082**

**removing**

    attributes, 355

    dependencies, 611-612

**renaming agents, 417-418**

**Report Operator role, 78**

**report parameters, 614**

**Report Security Administrator role, 78**

**report server, Registry keys, 1282**

**reporting, 204-206. See also reports**

    agents, 409-410

    CER, 799-800

    client monitoring, 819-823

    components, installation, 257-260, 262

    in design stage (deployment planning), 165

    Management Group ODR, 825

    ODRs, 824

    in OpsMgr 2007, 54, 88-89

    roles, creating Report Operator, 481-483

    security, 471

    SRS, testing, 258

    validation of, 319-322

Windows Error Reporting, 798-799

**Reporting Component, 46**

**Reporting Data Warehouse Server Component, 102**

**Reporting pane (Operations console), 131**

**Reporting section (management pack schema), 1164**

**Reporting Server, 103**

SSL, configuring, 525

updating with RMS location, 575

URL settings, 359

**reporting server clusters, installing, 455-457**

**Reporting Server Component, 225**

**reporting servers, hardware requirements, 154**

**Reporting space (Operations console), 362-365**

**reports, 46-49, 614. See also reporting**

ACS reports. *See also* audit reports

accessing, 767-770

backing up, 584

installing, 756-757

integration scenarios, 758-760

AEM, 211

for alerts, 627, 629-630

audit reports, 749. *See also* ACS reports

access to, 764

access violation scenario, 786-789

account management scenario, 784-786

archiving, 764

consumers of, 764

Forensic category, 784

Planning category, 783

policy changes scenario, 789-794

scheduling, 768-769

system integrity scenario, 794-795

backing up, 542, 583

creating in Visual Studio

data source views, 1204

data sources, 1203-1204

overview, 1202-1203

report creation process, 1207, 1209, 1211-1212

report models, 1203, 1206

emailing, 366, 1215-1216

for events, 627

exporting, 365

generic reports, 364-365

linked reports, 1198-1202

on network device performance, creating, 892-894

Operations console favorite reports, 1190-1191, 1193

output, creating, 1214-1215

overview, 1188

parameters for, 363-364

publishing, 1193, 1195-1197

report models

creating, 1203, 1206

deploying, 1206

saving, 365

scheduling, 365, 1214-1216

SRS (SQL Reporting Services), 582-583

targeted reports, 362-363

Top Applications report, 820

Top Error Groups report, 821-823

views versus, 47-48

**ReportServerTempDB database, backing up, 541**

**repromoting RMS clusters, 467**

**requesting certificates, 513-514**

**requirements, 92**

accounts, 490-491

business requirements, 140-141

comparison chart, 92-93

Dell management pack, 1259

functionality requirements in assessment documents, 140

hardware requirements

ACS Collector, 155

ACS database servers, 155

ACS Forwarder, 155

agents, 156

data warehouse servers, 155

gateway servers, 152-153

management servers, 151-152

multiple-server configuration example, 175

Operations console, 155

Operations database, 152-154

reporting servers, 154

- Root Management Server (RMS), 149-150
- System Center Essentials, 169
- two-server configuration example, 173
- Web console, 156
- installation requirements, 234-235
  - Operations console, 336-337
  - security accounts, 239
  - software requirements, 239-240
  - Windows, 236
- installing RMS clusters, checking, 459-460
- network connectivity requirements, 144
- operating system requirements, 156-159
- processing power requirements, 146
- remote agents, 385
- software requirements, 156-163
- technical requirements, 140
- trust, agent deployment, 402
- ReSearch This! Management Pack (RTMP), 1005-1007, 1308**
- resetting**
  - Administrator roles, 483-485
  - monitors, 686-687
- resolution states, 358, 716-718**
- resolve\_alerts.ps1 script, 1153**
- resolving alerts, 317-319**
- resource groups, 441, 458-460**
- resource kit utilities**
  - AD integration sample script, 730-731
  - downloading, 730
  - Effective Configuration Viewer, 731-733
  - Vista gadget bar, 733-736
- Resource Kits**
  - AEM, 843
  - online information, 1313
- resources, sharing among management groups, 104**
- restarting Health service, 1014**
- restoring, 576, 586**
  - clustered RMS, 576-577
  - Operations database, 564-565
  - RMS to management server, 572-576
  - resultant set of rules, viewing, 642-644
  - retention, 544
  - revision identifier (XML files), 1168
- RMS (Root Management Server), 71, 81, 100, 102, 203, 222, 224, 1058**
  - availability of, 108
  - clusters
    - ACS collector redundancy, 452
    - installing, 457-458, 460-467
    - repromoting, 467
  - connections, 338
  - downed RMS, disaster recovery from, 589
  - encryption keys
    - backing up, 255, 570-572
    - creating, 574
  - hardware requirements, 149-150
  - installation, 249-251, 253-254, 256
  - memory usage, 468
  - promoting management servers to, 589
  - restoring
    - clustered RMS, 576-577
    - to management server, 572-576
- RMS key, sharing, 463**
- role-based security, 75, 77-78, 471-474, 477**
  - Action account, 492
    - low-privileged accounts, 493-494
    - Management Server Action account, 493
    - modifying credentials, 496
    - MonitoringHost.exe process, 492
    - Windows 2000/XP, 495
    - Windows Server 2003/Vista, 495
  - Agent Installation account, 499
  - Computer Discovery account, 499
  - Config Service/SDK accounts, 496-499
  - Data Reader account, 500
  - Data Warehouse Write Action account, 499
  - Gateway Action account, 501-502
  - Health Service account, 501
  - Notification Action account, 499
  - required accounts, 490-491
  - Run As Accounts, 488-490
  - Run As Profiles, 487-488

user roles

creating, 477-483

resetting Administrator roles, 483-485

troubleshooting, 483

## **roles, 77, 100, 143**

assignments, 474

list of, 78

scopes, defining, 480

## **rollups, 116**

aggregate rollup monitors, 120, 682

dependency rollup monitors, 121, 682

health rollups, IIS management pack, 1255

## **ROM (Remote Operations Manager), 1047**

certificates, 1055-1056

Gateway Server Component, 1054-1055

grooming, 1076-1077

Master Host, 1060-1065

minimum requirements for, 1056-1058

monitoring customer network devices, 1073

online information, 1318

preparing operations manager for, 1065

Active Directory, 1065-1067

Certificate Authority, 1067-1070

DMZ, 1070

DNS, 1065-1067

firewalls, 1070-1072

installing Service Provider management pack, 1072-1073

RWW (Remote Web Workplace), 1058-1060

SMB service providers, 1050-1052

transition from OpsMgr, 1052

## **Root Management Server. See RMS**

## **RSA deployment approach (Ready, Shoot, Aim), 137**

## **RSKeyMgmt.exe utility, 584**

## **RTMP (ReSearch This! Management Pack), 1005-1007, 1308**

## **rule groups, 70**

## **rule overrides, 609**

## **rules, 119, 356, 602-603, 648-649**

AD\_Client\_Connectivity script parameters, 1299

AD\_Client\_GC\_Availability script parameters, 1300

AD\_Client\_PDC\_Response script parameters, 1300

AD\_Database\_and\_Log script parameters, 1296-1297

AD\_Essential\_Services\_Running script parameters, 1299

AD\_General\_Response script parameters, 1297

AD\_Global\_Catalog\_Search\_Response script parameters, 1297

AD\_Op\_Master\_Response script parameters, 1298-1299

AD\_Replication\_Monitoring script parameters, 1296

alert-generating rules, 649-653

collection rules, 653-662

Collect\_Mailbox\_Statistics script parameters, 1302

Collect\_Message\_Tracking\_Log\_Statistics script parameters, 1303

Collect\_Public\_Folder\_Statistics script parameters, 1302-1303

configuring, 1135-1136

cook down, 128-129

creating, 649, 1156-1157, 1159

custom SNMP rules, 877-878

creating, 880-894

SNMPUTIL.exe utility, 878-880

disabling, 356, 623, 629

finding in Operations console, 703-706

in HP Servers Management Pack for Operations Manager, 872

identifying, 630

monitors versus, 84, 897

overriding, 356, 629

resultant set of rules, viewing, 642-644

targeting, 595, 665-666

timed commands, 663-665

VerifyEAS script parameters, 1301

VerifyMAPI script parameters, 1301

VerifyMFR script parameters, 1300

VerifyOMA script parameters, 1301

VerifyOWA script parameters, 1301

## **Run As Accounts, 79, 360, 488-490, 640**

## **Run As Profiles, 78, 361, 487-488**

**running**

- Discovery Wizard, 294
- Migration Tool, 289-290, 292

**runtime tools for creating company knowledge, 700**

**RWW (Remote Web Workplace), 1058-1060, 1080-1082**

**S**

**SA (Software Assurance), 800**

**same hardware migrations, 281-283, 288-296**

**SAN (Storage Array Network), disk performance, 470**

**saved searches, 367**

**saving reports, 365**

**Savision Live Maps, 1123**

**SCADA (Supervisory Control And Data Acquisition), 829**

**scalability**

- of management groups, 187-188
- multiple-server configuration example, 176
- of OpsMgr 2007, 52

**scaling out, 1042-1043**

**scaling servers, 1042**

**scaling up, 1042, 1044**

**SCCP (System Center Capacity Planner), 166, 1024**

**scheduling**

- audit reports, 768-769
- backups, 542-544, 558-560
- computer discovery, 372-373
- reports, 365, 1214-1216

**schema files for management packs, 595**

**schema types, 607**

**SCOM (System Center Operations Manager), 12, 809**

**Scope feature (Operations console), 623**

**scopes, 143, 474**

- Operations console, 704-706
- roles, defining, 480

**SCP (service connection point), 388**

**screen capturing alert text, 698**

**“Script or Executable Failed to Run” alert, debugging, 1309**

**script rules, 657-662**

**scripting guide for Virtual Machine Manager, 1026**

**Scripting Guys, 1021**

**scripts**

- & (ampersand) in, 663
- for Configuration Manager, 1024
- property bags, definition, 1220
- resolve\_alerts.ps1, 1153
- SQLDBSize.vbs, 1217
- SQLDBUsedPercent.vbs, 1217
- SQLLogSize.vbs, 1217
- SQLLogUsedPercent.vbs, 1217

**SCVMM (System Center Virtual Machine Manager), 991, 1025, 1128**

**SDK (Software Development Kit)**

- accounts, 253, 496-499
- distributed applications versus, 987
- Operations Manager, 220
- security, 472
- stopping, 484

**SDK and Config Service account, 164**

**SDK service, 71, 79**

- explained, 106-107
- promoting management server to RMS, 576
- Registry keys, 1279-1280
- startup type, 465

**sdk\_users role, 502**

**SDM (System Definition Model), 23**

**sealed management packs, 89, 117, 596**

- creating, 614-615, 1223-1224
- disabling rules/monitors, 623
- updating, 596
- viewing, 634-635

**search feature in Operations console for network devices, 868**

**search results, viewing, 914**

**searches**

- for rules/monitors, 703-704
- saved searches, 367

**Secure Sockets Layer, 473**

**SecureStorageBackup tool, 254, 570-575****security, 739**

accounts, 164-165, 239

ACS, 526-527, 765

enabling certificate support, 528

encryption, 529

installing certificates, 527-528

agents, proxying, 511-512

connected management groups, 1100

for consoles, 75

databases, 502-503

firewalls, 529

agents, 532-533

configuring proxy settings, 534

ports, 530-532

Forefront, 1140

for Health service, 106

Health service lockdown tool, 525-526

least privilege, email, 1067

logs, 410

migration, management packs, 289

monitoring, 480

multiple domains, 218

mutual authentication, 503-507, 511

for RMS clusters, 460-461

role-based, 77-78, 471-474, 477

Agent Installation account, 499

Computer Discovery account, 499

Config Service/SDK accounts, 496-499

creating user roles, 477-478, 480-483

Data Reader account, 500

Data Warehouse Write Action  
account, 499

Gateway Action account, 501-502

Health Service account, 501

low-privileged accounts, 493-494

Management Server Action account, 493

modifying credentials, 496

MonitoringHost.exe process, 492

Notification Action account, 499

required accounts, 490-492

resetting Administrator roles, 483-485

Run As Accounts, 488-490

Run As Profiles, 487-488

troubleshooting user roles, 483

Windows 2000/XP, 495

Windows Server 2003/Vista, 495

of set commands (SNMP), 851

SSL, configuring, 525

**security adaptations, 1041-1042****security boundary in ACS, creating, 748-749****Security Event log, 739****security events**

determining number of, 747

network bandwidth utilization, 145

**security groups, creating ACS auditors security  
group, 753-754****security health monitors, 121****security model, management group design  
planning, 143****Security node (Administration space), 360-361****security policies, 741-742****security policy enforcement, OpsMgr 2007  
solutions to, 43-44****security regulations, online information on, 740****security settings**

on ACS database, 756

agents, 359

**selecting**

authentication, 253

management packs, 326

**self-tuning thresholds, 46, 83, 671-675****sending error reports to Microsoft, 247****server components, 81-82**design stage (deployment planning),  
148-156

ACS Collector, 155

ACS database servers, 155

ACS Forwarder, 155

agents, 156

data warehouse servers, 155

gateway servers, 152-153

management servers, 151-152

Operations console, 155

Operations database, 152-154

reporting servers, 154

- RMS (Root Management Server), 149-150
  - Web console, 156
- list of, 100-105
- network bandwidth utilization, 145
- operating system requirements, 156-159
- software requirements, 156-163
- Server Management Pack (Dell), 1116**
- Server Management Packs for OpsMgr 2007 (HP), 1114-1116**
- server OML, 159**
- servers. See also specific types of servers (e.g. ACS, RMS)**
  - ACS Collector Component, 227-228
  - ACS Database Server Component, 227
  - Data Warehouse Component, 226-227
  - Gateway Server Component, 224-225, 266-267
  - installation, 241
  - management
    - Action account, 492-496
    - configuring proxy settings, 534
    - installation, 256
    - mutual authentication, 503-507, 511
  - Management Server Action account, 493
  - Management Server Component, 224
  - Operations Database Component, 225-226
  - provisioning, 1042-1045
  - reporting components, installation, 257-260, 262
  - Reporting Server Component, 225
  - scaling, 1042
  - Windows, domain properties, 236
- service connection point (SCP), 388**
- service dependencies in assessment documents, 140**
- Service Design (ITIL v3), 27**
- Service Level Agreements (SLAs), 139, 819, 1049**
- Service Manager, 57-58**
  - integration with, 1029
  - online information, 1318
- service modeling, explained, 111-115**
- Service Modeling Language (SML), 23, 25, 111**
- service models, 51**
- Service Operation (ITIL v3), 27**
- Service Oriented Architectures (SOA), 1039**
- service packs, restoring databases, 565**
- Service Provider License Agreement (SPLA), 1060**
- Service Provider management pack, installing on ROM, 1072-1073**
- Service Provider Mode (System Center Essentials), 1078**
  - configuring, 1079-1080
  - installing RWW, 1080-1081
  - name resolution, 1079
  - obtaining certificates, 1079
  - outbound firewalls, 1079
- service providers (SMB), 1050-1052**
- Service Strategy (ITIL v3), 27**
- Service Transition (ITIL v3), 27**
- service-oriented monitoring, 71-72**
- services, 104**
  - accounts, requirements, 491
  - ACS. See ACS
  - Config Service account, 496-499
  - installing RMS clusters, creating, 461-462
  - list of, 79
  - Local Service accounts, 495
  - in Monitor Wizard, 676
  - SDK
    - accounts, 496-499
    - Operations Manager, 220
    - security, 472
    - stopping, 484
- sessions, starting capture sessions, 914**
- set commands (SNMP), security, 851**
- Set messages (SNMP), 846-847**
- SetSPN utility, 465**
- Setup Wizard, 255**
- SetupOM.exe, installation from, 234**
- severity values, 1138**
- SharePoint, integration with, 1029, 1031**
- SharePoint Monitoring Toolkit for OpsMgr, 1312**
- shares, creating hidden, 463**

**sharing**

- hardware, 80
- resources among management groups, 104
- RMS key, 463

**shortcuts to views, creating, 366****Silect MP Studio, 1183-1188**
**Simple Network Management Protocol.**  
 See **SNMP**
**simple recovery, 554, 557, 561****Simple Threshold monitor, 671-672****simulation, predicting behavior by, 905**
**single-management group design sample,**  
**198-199**
**single-server configuration example, 167-171,**  
**196-197**
**single-server Operations Manager**  
**installation, 241**
**size**

- of ACS database, managing, 778-780
- of Operational database, determining, 632
- of queue, 633

**sizing**

- limitations of, 178-189
- management groups, 430

**SLAs (Service Level Agreements), 139, 819,**  
**1049-1050**
**small and medium business, 1049**
**smaller-sized organizations, network**  
**management, 1048-1049**
**SMB (small and medium business), 1049****SMB service providers, 1050-1052****SMEs (subject matter experts), 228, 1092****SML (Service Modeling Language), 23, 25, 111**
**SMS (Microsoft Systems Management Server),**  
**21, 393-394, 801**
**SNMP (Simple Network Management Protocol),**  
**845-846, 850**

- architecture of, 846-848
- community names, 851
- custom monitors, 877-878
  - creating, 894-901
  - SNMPUTIL.exe utility, 878-880

 custom rules, 877-878
 

- creating, 880-894

## SNMPUTIL.exe utility, 878-880

## enabling, 851

## MIBs, 848-850

## monitors versus rules, 897

## network devices supporting, 877

## OIDs, 848-850

## polling conversation contents, 864

**SNMP devices, licensing, 161****SNMP Library, 376****SNMP monitor, 679-680****SNMP V2(c) standard, 76, 851-852****SNMPUTIL.exe utility, 878-880**
**SOA (Service Oriented Architectures), 1039**  
**software**

## AKM2XML resource kit utility, 1163

 Citrix Presentation Server Management  
 Pack, 1118-1119

## Dell Server Management Pack, 1116

## eXc software, 1121-1122

 HP Server Management Packs for  
 OpsMgr 2007, 1114-1116

## IBM Director Management Pack, 1118

## Jalasoft Xian IO, 1123-1127

## networks VMware Management, 1128-1130

## Quest Management Xtensions, 1128

## requirements

## comparison chart, 92-93

## server components, 156-163

## Savision Live Maps, 1123

## third-party connectors, 1112-1114

## Unisys ES7000 Management Pack, 1118

**software acquisition, software development**  
**versus, 65**
**Software Assurance (SA), 800**
**software containers (distributed**  
**applications), 950**
**software development, software acquisition**  
**versus, 65**
**software distribution in ConfigMgr 2007, 56****software errors, 14**



- software updates in ConfigMgr 2007, 55
- space utilization of databases, 629
- spaces, 343
- SPLA (Service Provider License Agreement), 1060
- SQL 2005 Reporting Services, changing log file location, 322
- SQL Database Space Report, 194
- SQL Report Manager, ACS administration, 769-770
- SQL Reporting components, installation location, 455
- SQL Reporting Services (SRS), 258, 582-583
  - encryption keys, backing up, 584-585
  - ReportServer database, backing up, 541
- SQL Server 2005
  - clusters, installing, 443-447
  - editions, ACS and, 86
  - memory usage, 468
  - truncating transaction log, 563
- SQL Server 2005 Enterprise edition for ACS deployment, 751
- SQL Server 2005 Standard edition for ACS deployment, 751
- SQL Server databases
  - backing up, 553-554
    - steps in, 554-560
  - truncating transaction log, 560, 562-563
  - OpsMgr databases on, 152
  - restoring, 564-565
- SQL Server management pack, 629
  - installation, 1249-1250
  - object discovery, 1250-1251
  - tuning and alerts, 726-727, 1251-1253
- SQL Server named instances, ACS connections, 751
- SQL Server service, startup mode, 447
- SQLDBSize.vbs script, 1217
- SQLDBUsedPercent.vbs script, 1217
- SQLLogSize.vbs script, 1217
- SQLLogUsedPercent.vbs script, 1217
- SqlSpec utility, 570
- SRS. See SQL Reporting Services
- SRS Recovery Planning, online information, 1308

- SSL (Secure Sockets Layer), 473
  - configuring, 525
  - monitoring, troubleshooting, 1258
  - recording, 909
- standalone CA, 515-517
- standard datasets, 548
- standard OML, 159
- StandardDatasetAggregation table (data warehouse), 547-548
- standarddatasetgroom stored procedure, 549
- standarddatasetmaintenance stored procedure, 549
- Standardized level (IO Model), 34
- starting capture sessions, 914
- starting clean, 278-281
- startup mode for SQL Server service, 447
- startup type for SDK service, 465
- state, 51
  - agent-managed, 374, 378, 380
  - agentless managed, 380-382, 404-408
  - monitors, 604, 719
  - unknown, 384
- state changes, 128
- state icons for monitors, 120
- state machines, 120
- state monitoring rules, 872
- state-based management, explained, 117
- states, health state, 69
- static membership, 1017
- Static Thresholds monitor, 669-672
- status, 812
- Stirling, 1140
- stopping SDK services, 484
- Storage Array Network (SAN), disk performance, 470
- stored procedures for grooming databases, 549
- sub-elements (of management packs), 606
- subject matter experts (SMEs), 228, 1092
- subscriptions, 361
  - categories and troubleshooting, 692
  - creating, 689, 695-699
- summarizing migration, 295-296
- Supervisory Control And Data Acquisition (SCADA), 829

**Supporting quadrant (MOF), 30**  
**surveys, errors, 818-819**  
**swing server approach, new hardware/same hardware migrations, 287-288**  
**synthetic transaction monitoring, 804, 829, 843**  
     applications, 940-947  
     databases, 922-923, 925-928  
     Exchange, 933-935, 939-940  
     ports, 928, 930, 932-933  
     simulation, predicting behavior by, 905  
     watcher nodes, 906-907  
     Web applications, 907-909, 912-920  
**Synthetic Transactions Library, 377**  
**Syslog messages, capturing, 1135-1137**  
**System Cache, memory usage, 468-469**  
**System Center**  
     intent of, 25  
     online information, 1317-1318  
     products in, 54  
     reporting in, 54  
**System Center Capacity Planner, 59, 166, 1024**  
**System Center Configuration Manager, 55-56, 393, 1022**  
**System Center Core Library, 377**  
**System Center Core Monitoring, 377**  
**System Center Data Protection Manager 2007, 58-59**  
**System Center Essentials, 53, 56, 1047-1048, 1052-1054**  
     ConfigMgr 2007 versus, 96  
     evaluation copy, 94  
     installing on customer networks, 1074  
         configuration options, 1076-1078  
         OpsMgr management groups, 1075-1076  
     minimum installations, 1077-1078  
     Network Device Monitoring Library, 865-871  
     online information, 1317-1318  
     OpsMgr 2007 versus, 94-95  
     Service Provider Mode, 1078-1081  
     single-server configuration example, 167-169  
**System Center Internal Library, 377, 616**

**System Center Internal Task Library MP, 640-641**  
**System Center Operations Manager (SCOM), 11, 809**  
**System Center Operations Manager Migration Wizard, 290**  
**System Center Pack Catalog, 616, 1164, 1310**  
**System Center Roadmap, 1317**  
**System Center Rule Templates, 377**  
**System Center Service Manager, 57-58, 1029**  
**System Center Task Templates, 377**  
**System Center UI Executed Tasks, 377**  
**System Center Virtual Machine Manager (SCVMM), 59, 991, 1025, 1128**  
 system databases, user databases versus, 540  
**System Definition Model (SDM), 23**  
**System Error Group view, 814**  
**System Hardware Library, 377**  
 system integrity scenario (audit reports), 794-795  
**System Library, 377**  
 system maintenance, 1035, 1037-1038  
     antivirus software, 1037  
     disk backups, 1037  
     disk defragmentation, 1035-1036  
     patch management, 1036-1037  
 system outages, reasons for, 14-15  
 system requirements, comparison chart, 92-93  
 system-level management of ACS  
     database, 765  
**SystemCenterForum, 1120, 1220**  
**Systems Management Server (SMS), 21, 393-394, 801**

## T

**targeted reports, 362-363**  
**targeting**  
     monitors, 123, 665-666  
     rules, 595, 665-666  
**task overrides, 610**

## tasks, 71, 119, 604

- agent tasks, 1018
- console tasks, 613, 1018-1021, 1149-1153
- context menu tasks, enabling, 1292
- creating, 356
- diagnostic tasks, 1008-1010
  - console tasks and, 1019-1021
  - creating, 1009, 1011-1012
- embedding in alert details, 688
- Enable Audit Collection task, running, 760-762
- in management packs, 601-602
- recovery tasks, 1008-1010
  - console tasks and, 1019-1021
  - creating, 1013-1014
  - restarting Health service, 1014

## TCO (Total Cost of Ownership), 800

## TCP (Transmission Control Protocol), port monitoring, 1131-1135

- creating, 930-932
- viewing performance, 932-933

## TCP Port template, 352

## technical requirements in assessment documents, 140

## tempdb, location of, 470

## templates, 90, 612-613

- certificate, creating, 513
- importing into Local Security Policy, 743
- management pack templates, 352
- policies, 809
- Web Application Management Pack Template, 1256-1258

## Templates section (management pack schema), 1164

## Terminal Services Farm templates, 996-998

## terminology changes in OpsMgr 2007, 69-71

## test environments

- for management packs, 631
- production environments versus, 143

## testing

- cluster failover, 442-443
- connections, 919

## crashes/hangs, 810

- email format, 690
- RMS clusters, 466-467
- SRS, 258
- TCP ports, 931

## text, screen capturing, 698

## third-party management packs, 1114

- Citrix Presentation Server Management Pack, 1118-1119
- Dell Server Management Pack, 1116
- HP Server Management Packs for OpsMgr 2007, 1114-1116
- IBM Director Management Pack, 1118
- Unisys ES7000 Management Pack, 1118

## third-party product connectors, 1112-1114

## thresholds (monitors), changing, 629

## tiered management groups, 1098-1099

## time sensitivity, 674

## timed commands, 603, 663-665

## timed scripts, memory leaks, 620

## Tivoli, 871, 1110-1112

## toolbar, converting navigation button area (Operations console) to, 132

## tools

- Command Shell, 221
- ConfigureEventLogs, 411
- Health service lockdown, 525-526
- for measuring service, 1049-1050
- Migration Tool, running, 289-290, 292
- MOMCertImport, 513, 517-519
- ports, 420
- Secure Storage Backup, 254

## Top Applications report, 820

## Top Error Groups report, 821-823

## Total Cost of Ownership (TCO), 800

## total loss, disaster recovery from, 586-587

## tracing, diagnostic, 645

## tracking SLAs, 819

## training courses, online information, 1307

## training videos, online information, 1312

## transaction logs

- backups, effect on, 561
- truncating, 556, 560, 562-563

- transactions, 561
- transitory alerts, 315
- Transmission Control Protocol. *See* TCP
- trap destinations, 852
- Trap messages (SNMP), 846-847
- trap receivers, 847
- trap sending, enabling, 852
- trap-based alert rules (SNMP), creating, 880-887
- trap-based detection monitors (SNMP), creating, 898-901
- trap-based event rules (SNMP), creating, 886-888
- traps (SNMP), collecting, 880
- trekking, 204-206
- trigger-only flags, 608
- troubleshooting
  - agents, 418-422
  - ASP.NET installation, 249
  - CA, 519-520, 523
  - clients, monitoring, 211
  - data warehouse, 321-322, 576
  - discovery process, 372
  - DNS, 624
  - Event ID 26319, 497
  - Exchange 2003 management pack, 1237
  - importing management packs, 638
  - installation, 273-275
  - management packs, 630-634
  - Microsoft.interop.security.azure.dll, 250
  - migration, 299-300
  - MOM 2005 SharePoint WebPart, 1030
  - OWA logon failure, 1244-1246
  - SSL monitoring, 1258
  - subscriptions and categories, 692
  - user roles, 483
  - watcher nodes, 906
  - Web Page views in Web console, 359
- truncating transaction logs, 556, 560, 562-563
- trust requirements, agent deployment, 402
- trusted authentication, running Operations console without, 340-342

## tuning

- Active Directory management pack, 1230-1235
- alerts, 718, 723
  - Active Directory management pack, 724-725
  - by color, 718-719
- Exchange Server 2003 management pack, 723-724
- SQL Server management pack, 726-727
- Windows Server Operating System management pack, 726
- Dell management pack, 1259-1260
- Exchange 2003 management pack, 1237-1249
- IIS management pack, 1255
- management packs, 622-631
- performance counters, 180
- SQL Server management pack, 1251-1253

## two-server configuration example, 170-174

## Type override, 610

TypeDefinitions section (management pack schema, 1163)

# U

## UI page sets, 613

## UI pages, 613

## UNC (Universal Naming Convention), 799

## Unified Messaging role (Exchange 2007), 1031

## uninstalling

- management packs, 598
- OOMADS, 285

## Unisys ES7000 Management Pack, 1118

## unit monitor types, 608

## unit monitors, 119, 123-126, 604, 681, 1182

## Universal Naming Convention, 799

## unknown state, 384

## unlocking Action accounts, 526

## **unsealed management packs, 596**

- backing up
  - with Operations console, 580-582
  - with PowerShell scripts, 577-580
- exporting, 634-635

## **untrusted domains, entering credentials, 338**

### **updating**

- domains, accounts, 495
- management packs, 90, 616
- Reporting Server with RMS location, 575
- sealed management packs, 596
- Web Console Server with RMS location, 575

### **upgrading. See migration**

### **URL settings, 359**

### **user accounts**

- in Exchange 2007, creating, 1032
- provisioning, 1040-1041

### **User Accounts Created and User Accounts Deleted report, 786**

### **user applications, design stage (deployment planning), 164**

### **user community (RTMP), 1005-1007**

### **user databases, system databases versus, 540**

### **user errors, 15**

### **user notifications, 165**

### **user roles, 360, 1090-1091**

### **user-interface tier (distributed applications), 950**

### **users**

- adding, 480
- roles
  - creating, 477-478, 480-483
  - resetting Administrator roles, 483-485
  - troubleshooting, 483

### **utilities**

- on installation media, 332
- ports, 420

## **V**

### **validating**

- clusters, 441
- email format, 690
- management groups, 304-305
  - Active Alerts view, 315-317
  - distributed application Diagram view, 311-313
  - distributed application Health Explorer, 309-311
  - distributed application Performance view, 314-315
  - distributed application PowerShell integration, 313-314
  - global views, 307-309
  - Operations console installation, 305-307
  - reporting function, 319-322

### **value-add features, customer computers and networks, 1089-1093**

### **VerifyEAS script parameters, 1301**

### **verifying**

- management packs
  - installation, 639-640
  - with MPVerify utility, 615
- servers, 503

### **VerifyMAPI script parameters, 1301**

### **VerifyMFR script parameters, 1300**

### **VerifyOMA script parameters, 1301**

### **VerifyOWA script parameters, 1301**

### **version checking, disabling in Registry, 66**

### **version numbers (XML files), 1169**

### **versions**

- management packs
  - converting MOM 2005 management packs, 619-621
  - determining, 617-619
- Volume License, 279

### **vertical scaling, 1042, 1044**

### **view types, 613**

**viewing**

- alerts, 41-43
- connected data, 1106
- CSV files in Microsoft Excel, 713
- historical information, 44-49
- management packs, 641
- ODBC data source, 752
- overrides, 610
- performance
  - OLE DB, 928
  - TCP ports, 932-933
- product knowledge, 49-50
- resultant set of rules, 642-644
- sealed management packs, 634-635
- search results, 914
- websites, performance data, 920
- XML files, 1166-1168

**views, 45, 356, 614**

- Active Alerts view, 315-317
- alert views, creating, 720-723
- Application, 813
- Application Error Group, 813
- consoles, AEM, 812-814
- Crash Listener, 814
- creating, 626, 1154, 1156
- dashboard view, creating, 347-349
- data source views, creating, 1204
- Diagram view for distributed applications, 311-313
- Distributed Application Diagram, 947
- Exchange Service, distributed applications, 964-965
- global views, 307-309
- My Views, creating, 366
- Performance view for distributed applications, 314-315
- Personalize view, 345-346
- pivoting, 311
- reports versus, 47-48
- shortcuts, creating, 366
- System Error Group, 814

- Web Applications State view, 973

- Web Page view

- creating, 346-347
  - in Web console, 359

**Virtual Machine Manager, 59, 1139**

- integration with, 1025-1026
- management pack, 1043

**virtual machines**

- backing up, 1037
- online information, 1309

**virtual RMS, creating, 464-465****virtual server clusters, 443, 1308****virtualization**

- components, 229-231
- of disaster recovery, 589
- in Windows Server 2008, 1045

**Vista gadget bar, 733-736****Visual Studio**

- creating reports
  - data source views, 1204
  - data sources, 1203-1204
  - overview, 1202-1203
  - process for, 1207-1212
  - report models, 1203, 1206
- DSI integration, 23

**Visual Studio Tools for Office (VSTO) Second Edition, 339, 700, 1313****VMWare, integration with, 1034****VMware Management (nworks), 1128-1130****Volume License version, 279****VSTO (Visual Studio Tools for Office) Second Edition, 339, 700, 1313**

## W

**Watchanator, 1018****watcher nodes, 85, 311, 906-907****WCF (Windows Communication Foundation), 472**

**Web Application Editor, 912**

**Web Application Management Pack Template, 1256-1258**

**Web Application Monitoring Library, 378**

**Web Application template, 352**

**web applications**

creating with Internet Explorer Service templates, 973-976

monitoring, 907-909, 912-920

**Web Applications State view, 973**

**web browsers, viewing XML files in, 1166**

**Web console, 73, 103, 132**

hardware requirements, 156

performance counters, 1269

refresh interval, 366

URL settings, 359

Web Page views in, 359

**Web Console Component, 228**

**Web Console Server, 212**

redundancy, 458

updating with RMS location, 575

**Web Page view**

creating, 346-347

in Web console, 359

**webcasts, creating rules, 649**

**WebParts, troubleshooting MOM 2005**

**SharePoint WebPart, 1030**

**websites, 1305**

advanced monitoring, configuring, 912-919

MVLS, 279

performance, viewing, 920-921

performance counters for, 908

**Windows**

Action accounts, 495

domain properties, 236

security accounts, 239

**Windows Client Operating Systems Library, 378**

**Windows Cluster Library, 378**

**Windows Communication Foundation (WCF), 472**

**Windows Computer group type, properties, 1017**

**Windows Core Library, 378**

**Windows Error Reporting, 798-799**

**Windows Events monitor, 668, 681-686**

**Windows Explorer Data Source Service DA, creating, 982-984**

**Windows Explorer Data Source Service templates (Enterprise Health Monitoring), 980**

creating OLE DB Data Sources, 980-981

creating Windows Explorer Data Source Service DA, 982-984

customizing Data Source Service DA, 984-986

**Windows Internet Explorer Service DA, creating, 976-980**

**Windows Management Instrumentation, 16**

**Windows Performance Counters monitor, 668-675**

baselines, 673-675

self-tuning thresholds, 671-672

Static Thresholds monitor, 669-672

**Windows Registry, 1271**

**Windows Server 2008 virtualization, 1045**

**Windows Server Operating System management pack, tuning, 726**

**Windows Server Update Services (WSUS), 23, 1074**

**Windows Service Library, 378**

**Windows Service monitor, 675-678**

**Windows Service template, 352**

**Windows services, 104**

Audit Collection service, 108

Audit Forwarding service, 107

Config service, 107

Health service, 105-106

SDK service, 106-107

**Windows SNMP trap provider, 680**

**WMI (Windows Management Instrumentation), 16**

**WMI event and performance monitors, 680**

**work stoppages, cost of, 802**

**workflows, 602**

cook down, 128-129

data types, 129

diagnostics, 604

discoveries, 603-604

explained, 126-129

module types, 126-127

- monitors, 604
- recoveries, 605
- rules, 602-603
- tasks, 604

- workgroups, monitoring agents, 208**
- workgroupsmains (OpsMgr), 506-507, 511**
- write action module type, 127-128, 608**
- write action modules, 602**
- write actions, 927**
- WS-Management specification, 22, 76**
- WSUS (Windows Server Update Services),  
23, 1074**

## X–Z

- x.509 certificate authentication, 432**
- Xian IO (Jalasoft), 1123-1127**
- XML (eXtensible Markup Language), 1161**
  - converting management packs to, 90
  - management pack creation, 1170-1175
  - overview, 1161-1162
  - sample management pack XML file,  
1165-1170
  - XML documents
    - management pack structure, 1163-1164
    - viewing, 1166-1168
- XML Notepad**
  - online information, 1312
  - viewing XML files in, 1166, 1168
- Zerger, Pete, 1220**