

Chris Amaris
Tyson Kopczynski
Alec Minty
Rand Morimoto

Technical Edit by Guy Yardeni

Microsoft® System Center Enterprise Suite

UNLEASHED



SAMS

Microsoft® System Center Enterprise Suite Unleashed

Copyright © 2010 by Pearson Education, Inc.

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 authors 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: 978-0-672-33319-4

ISBN-10: 0-672-33319-8

Library of Congress Cataloging-in-Publication Data

Microsoft System Center Enterprise suite unleashed / Chris Amaris ... [et al.].
p. cm.

Includes bibliographical references and index.

ISBN-13: 978-0-672-33319-4 (alk. paper)

ISBN-10: 0-672-33319-8 (alk. paper)

1. Integrated software. 2. Information technology—Management. I. Amaris, Chris.
QA76.76.I57M498 2010
005.5—dc22

2010006460

Printed in the United States of America

First Printing April 2010

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 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@pearson.com

Editor-in-Chief

Karen Gettman

Executive Editor

Neil Rowe

Development Editor

Mark Renfrow

Managing Editor

Kristy Hart

Project Editor

Betsy Harris

Copy Editor

Karen Annett

Indexer

Erika Millen

Proofreader

Williams Woods

Publishing

Technical Editor

Guy Yardeni

Publishing

Coordinator

Cindy Teeters

Book Designer

Gary Adair

Compositor

Nonie Ratcliff

Contributing Writer

Robert Jue, MCP+I
2.0, MCSE, MCDBA,
MCTS

Introduction

The System Center family of products from Microsoft has undergone quite the evolution over the past decade, with some products purchased through acquisitions, to other products evolving from earlier releases that didn't work all that well, to what is now a very broadly deployed management suite of products. In 2009, the System Center products crossed that magical \$1-billion mark in revenues for Microsoft that signifies a product line has "made it" among the mass of products churned out of Redmond, Washington, every year.

This book covers real-world experiences with the System Center products, not like a "product guide" simply with step-by-step installation and feature configurations, but with real-world notes, tips, tricks, best practices, and lessons learned in the design, planning, implementation, migration, administration, management, and support of the System Center technologies based on years of early adopter and enterprise production deployments.

The 19 chapters of this book are written to highlight the most important aspects of the technologies that make up the System Center family of products. To combine the products into groups of technologies, this book covers the following:

- ▶ **Introduction**—The first chapter of this book provides an introduction to the System Center family of products, what they are, what they do, and what business and IT challenges they solve. The introduction paints the picture of what the rest of the book will cover and how you as the reader can jump to those sections of the book most important to you in your day-to-day IT management tasks.
- ▶ **System Center Configuration Manager 2007**—The first product covered in this book is the System Center Configuration Manager 2007 (SCCM) product, which is a product that has come a long way in the past decade. The earlier releases of Configuration Manager went by the name SMS, or Systems Management Server, which was known to take full-time personnel to manage the management system. However, now easily three to four generations later, SCCM with its latest R2 and service pack has really helped organizations with the patching, updating, imaging, reporting, and compliance management of their client and server systems. The four chapters in this book that cover SCCM address the planning and design process of implementing SCCM in an enterprise, the implementation of the product, and, more important, how administrators use SCCM to image, update, manage, and support the servers and client systems in their environment.
- ▶ **System Center Operations Manager 2007**—The second product covered in this book is the System Center Operations Manager 2007 (SCOM) product, which provides monitoring and alerting on servers and client systems. Rather than waiting for users to alert the help desk that a server is down, SCOM proactively monitors systems and provides alerts before systems fail, plus it logs error events and system

issues to help organizations address system problems—usually before they occur. The chapters dedicated to SCOM cover the planning and design of SCOM, the rollout and implementation of servers and monitoring agents, and the best practices on how to understand errors and alerts that allow IT administrators to be more proactive in managing their servers and the systems in their environment.

- ▶ **System Center Data Protection Manager 2010**—System Center Data Protection Manager 2010 (DPM) is a relatively new addition to the Microsoft management family of products. As traditional tape backups have been replaced by digital snapshots and digital data backups of information, DPM provides organizations the ability to have backup copies of their data. DPM incrementally backs up information from servers so that instead of backing up information once a night, DPM makes backups all day long for faster backup times and more granular recovery windows. This book covers the planning, design, implementation, and general recovery process of file systems, Microsoft Exchange, SharePoint Server, and SQL using DPM 2010.
- ▶ **System Center Virtual Machine Manager 2008**—In the past couple of years, virtualization has gone from something that was only done in test labs to data centers that are now fully virtualized—enabling organizations to have more than one server session running on a physical server system, and sometimes upward of 10 or 20 server sessions running on a single system. With the huge growth in virtualization in the data center, Microsoft released three major updates to the System Center Virtual Machine Manager (VMM) product in two years to address the needs of the enterprise. The two chapters dedicated to VMM go beyond the installation and setup of VMM 2008, and get into core components of the product that help organizations manage virtual guest sessions running on both Microsoft Hyper-V virtualization as well as VMware, and also how to convert physical servers to virtual servers (P2V), delegate the ability to administer and manage guest sessions, and the ability to share virtual host resources with users and administrators in the enterprise.
- ▶ **System Center Service Manager 2010**—After more than five years in development and many, many months in production deployment to fine-tune the product, Microsoft now has a help desk/incident management/asset life-cycle management/change management product called System Center Service Manager 2010 (SCSM). Being involved with the development of SCSM from its inception, the authors of this book have shared years of experience, tips, best practices, and lessons learned in the deployment, information tracking, reporting, and support of the SCSM product. SCSM brings together the information gathering, reporting, alerting, and knowledge-base information in the other System Center products into a single product that will help organizations better manage their IT infrastructures.
- ▶ **System Center Capacity Planner**—System Center Capacity Planner (SCCP) is not one of the products that organizations hear much about compared with the mainstream products like SCCM, SCOM, DPM, and VMM; however, SCCP adds a lot of value to an organization looking for a comprehensive set of tools to manage their environment. SCCP monitors the state of running systems as well as models the

planned operations of a future environment and provides IT architects and designers the information they need to properly size, procure, and deploy systems with the appropriate capacity needed to meet the needs of the organization. A single chapter is dedicated to SCCP and is content that is intended to help IT professionals better leverage a tool that is part of the System Center family of products.

- ▶ **System Center Mobile Device Manager**—System Center Mobile Device Manager (MDM) was just a simple plug-in tool a few years ago that helped organizations inventory and manage their mobile devices. With the growth in sophistication of the mobile phone—with business applications installed on the mobile devices along with the proliferation of phones where some users use their mobile phone as their primary “client device”—the need to manage the mobile devices becomes ever so important for an organization. The chapter in this book dedicated to MDM covers how to use MDM to asset track, remotely secure, patch and update, and support mobile devices in the enterprise.
- ▶ **System Center Essentials 2010**—The final chapter in this book covers the System Center Essentials 2010 (SCE) product, which is an all-in-one version of the product intended for organizations with fewer than 500 users and 50 servers. Rather than buying and implementing SCCM, SCOM, and VMM as separate individual products for a small or medium enterprise, SCE allows an organization to take advantage of the key components of the full-blown System Center products, but with much better ease as SCE leverages wizards, autoconfiguration components, and other features to simplify the management tasks of a smaller enterprise.

It is our hope that the real-world experience we have had in working with the entire System Center family of products and our commitment to relaying to you information that will be valuable in your planning, implementation, operation, and administration of System Center in your enterprise will help you more quickly gain and receive benefits from these managements tools from Microsoft!

CHAPTER 1

Introduction to the System Center Suite

System Center, which is licensed either individually or as a bundled suite, is a series of tools that help organizations manage their servers, client systems, and applications to be more proactive in responding to the needs of the IT data center. In fact, the name System Center actually didn't come about until just a few years ago; prior to that, the products were all sold separately.

Like with many families or suites of products, the first rendition of the suite is nothing more than a bunch of disparate products bundled together under a common brand name, but really have no integration in working together. System Center was no different—with the first couple of years of the product line being nothing more than name and branding.

Today, however—three to four years and two to three versions later—the System Center products actually do work better together and an IT organization can leverage information in the various System Center components more easily and for a common benefit.

This chapter introduces the System Center family of products, what the components are, and how the balance of the chapters in this book provide tips, tricks, best practices, and guidance on how to best leverage System Center in the enterprise.

What Is System Center?

As mentioned at the start of this chapter, System Center is a family or suite of management tools from Microsoft; being a family of tools, you don't go out and buy Quantity 1 of

IN THIS CHAPTER

- ▶ What Is System Center?
- ▶ Understanding System Center Configuration Manager
- ▶ Understanding System Center Operations Manager
- ▶ Understanding System Center Data Protection Manager
- ▶ Understanding System Center Virtual Machine Manager
- ▶ Understanding System Center Service Manager
- ▶ Understanding System Center Capacity Planner
- ▶ Understanding System Center Mobile Device Manager
- ▶ Understanding System Center Essentials
- ▶ Understanding System Center Licensing

System Center. Rather, you choose to buy an individual System Center component like System Center Configuration Manager 2007 for patching and updating systems, or you buy a licensed bundle of the main four products that Microsoft calls the System Center Management Suite and separately download and install additional System Center components that are outside of the licensed bundle for even more functionality. More details on the software licensing of the System Center products can be found in the section “Understanding System Center Licensing” later in this chapter.

Systems Management in the Enterprise

For years, IT departments have struggled with managing their servers and client systems, and hundreds of companies have arisen that provide tools for patching computer systems, imaging workstations, pushing out new software, monitoring servers and network devices, and backing up systems. However, over the years, organizations have found that each individual product would require a separate server, a separate set of policies or rules setup, a separate agent to be installed on the computer system, and a separate set of tasks to inventory the systems all doing similar things. With several different products installed on a system and no real sharing of information between the management agents and tools, enterprise systems management has been quite a clumsy process.

As an example, an organization would inventory its systems for asset tracking with one product to keep track of corporate assets. With a separate product, the organization would put an image onto its system. Yet another product would be used to patch and update the system. Another product would monitor the system and alert the administrators of a problem; this monitoring program would typically have to inventory the system to know what hardware and software it is monitoring and managing. The organization would have yet a completely different product to track help desk calls and problem tickets, in some cases capturing asset information from one of the other two tools mentioned earlier in this paragraph, but frequently the help desk tool would have its own management components to remotely control and support the user and system. Finally, the organization would have a separate product to back up data on the system, plus yet another separate product to provide security management of the system for security policies and controls.

With all this going on for just a single system, there's no wonder why systems management has been a dirty word in the computer industry. Everyone knows they need to do something about it, but when you try to do something about it by going out and getting the best-of-breed product from each vendor in the industry, you have 5 or 10 different products all vying to do some type of management of the system. Naturally, with that many different products doing different but similar things, changes made by one of the 5 or 10 products frequently would cause problems with one of the other components—setting the organization's systems management efforts back a step at a time.

Five to eight years ago, Microsoft provided tools for systems to do patching, monitoring, asset inventory, backup, and the like, but no better than the 5 to 10 separate vendor products, Microsoft tools were all separately installed, configured, and managed. Microsoft Systems Management Server (SMS) has a bad name in the industry for old-timers who tried to use the system years ago as even within this tool itself, it installed several separate agents on a computer to try to “help” the system monitor and manage updates, software

installation, inventory tracking, and remote control, with the SMS components themselves frequently conflicting and causing system problems.

Roll forward several years, and Microsoft combined all of their products under a single brand called System Center and has spent the past half of a decade getting the products to work together. Three or four generations later under the System Center brand, Microsoft now has tools that work together so an organization that buys a suite license isn't just buying a bundle of separate products, but a family of products that work together.

The whole premise of this book is how organizations can deploy the separate System Center components and then ultimately tie them together so that there is a coordinated effort from cradle to grave on a system that can be imaged, deployed, patched, updated, maintained, supported, and retired under a common management process. It's the full life cycle of a server or client system that is addressed in this book.

System Center Family of Products

In looking at the cradle-to-grave life cycle, how the System Center products fit in, and how the various chapters in this book cover the topics, the family of products are as follows:

- ▶ **System Center Configuration Manager**—System Center Configuration Manager (SCCM) starts with the ability of imaging or laying down the base operating system on a server or client system based on specific organizational guidelines for configurations. Once the operating system has been installed, SCCM continually patches and updates the system as well as provides the ability to push out new software to the system, also based on specific templates and guideline configurations. SCCM keeps track of system inventory, provides remote-control capabilities, and provides IT administrators the ability to ensure the system configuration is maintained in a common configuration.
- ▶ **System Center Operations Manager**—Once SCCM lays down the base configuration of the system and keeps it patched and updated, System Center Operations Manager (SCOM) takes over for monitoring the ongoing health of the system as well as the applications installed on the system. Specific rules are created that track the normal operations of the system, and any time the system falls out of the standards, the organization's IT personnel are notified of the changes.
- ▶ **System Center Data Protection Manager**—Although SCCM and SCOM deploy and monitor system operations, there are times when data is corrupted or lost or systems fail and having a backup of the data is crucial. This is where Data Protection Manager (DPM) fits in as it backs up client systems, server file systems, Exchange databases, SharePoint data, or SQL databases on a continuous basis, providing an organization the ability to recover a single lost or corrupted file all the way through restoring a completely dead system.
- ▶ **System Center Virtual Machine Manager**—As the industry has shifted from one made up of primarily physical server systems to one where servers are now virtualized in the data center, the Virtual Machine Manager (VMM) product from Microsoft helps organizations manage their virtual systems. In the fully managed scenario, in

the event that SCOM identifies a physical or virtual system is about to fail, it can automatically create a new guest session using SCCM to a Hyper-V or VMware virtual host, build out a brand-new system, and use DPM to automatically restore the latest backup of information all as a scripted disaster recovery process. VMM can also transfer fully running physical servers and transfer the operating system, application, and data to a virtual server in an automated physical-to-virtual (P2V) conversion process.

- ▶ **System Center Service Manager**—Although all of the previous tools chug along doing IT-related tasks, such as imaging, patching, monitoring, and backing up, organizations also have a need to manage processes and change control. The System Center Service Manager (SCSM) product is an incident management and change-control system that tightly integrates with SCOM, SCCM, and VMM to take alerts, automatically log the problems, take inventory information, and track system configurations so that help desk personnel and support individuals have at their fingertips information they need to support users and application owners in the enterprise. SCSM brings together management policies and processes as the umbrella under which the other System Center tools facilitate day-to-day tasks and procedures.
- ▶ **System Center Capacity Planner**—As an organization looks to replace servers and systems, or upgrade and deploy new software applications, the System Center Capacity Planner helps the organization test performance demands on current systems and model the future environment relative to the necessary hardware specifications needed to meet the performance demands of the organization.
- ▶ **System Center Mobile Device Manager**—Throughout an enterprise, an organization doesn't have just servers and client workstations, but the proliferation of mobile devices make up the IT landscape. System Center Mobile Device Manager (MDM) integrates with SCCM to provide cradle-to-grave management of mobile devices similar to what SCCM does for servers and client systems, including provisioning, updating, securing, monitoring, and wiping devices in the course of a mobile device's life cycle.
- ▶ **System Center Essentials**—Finally, not all enterprises have separate IT groups handling servers, client systems, and applications, such as enterprises with fewer than 500 users and fewer than 50 servers. Microsoft has System Center Essentials that provides key management functions around tracking inventory, patching and updating systems, deploying software, monitoring, and managing virtual systems that helps smaller enterprises meet their management needs in an all-in-one integrated tool.

Each of the products have had variations over the years (2003, 2007, 2008, R2, SP1, SP2, 2010, and so on) with each successive version adding more functionality and capabilities than the version before it. The balance of this chapter details each of the System Center products and provides a snapshot of what to expect throughout the chapters of this book.

Understanding System Center Configuration Manager

The first product covered in this chapter is the System Center Configuration Manager (SCCM) product shown in Figure 1.1; the current rendition is System Center Configuration Manager 2007 R2 SP2. SCCM is the start of the life cycle that deploys a system's operating system as well as installs the applications onto a server or client system, and then it keeps the system patched and updated all based on common templates the IT department creates to ensure standardization from system to system.

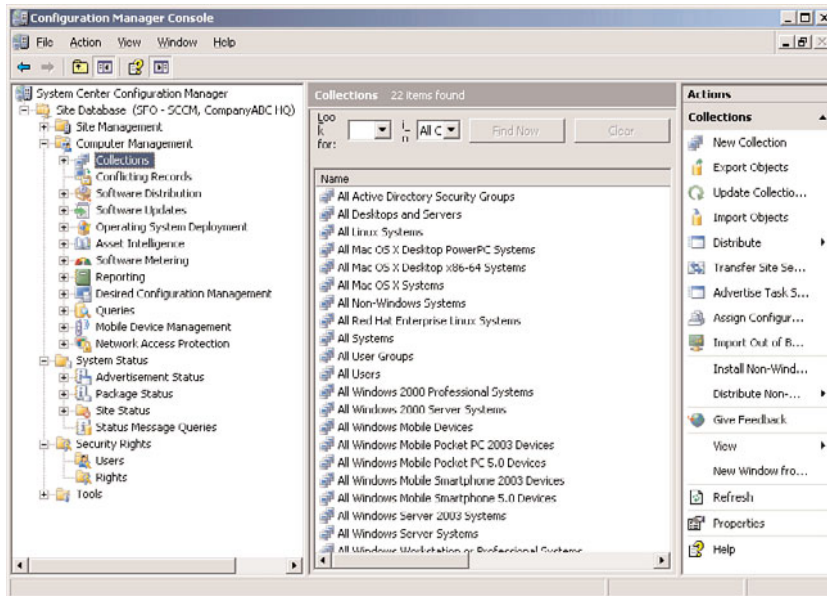


FIGURE 1.1 The System Center Configuration Manager console.

Business Solutions Addressed by System Center Configuration Manager

System Center Configuration Manager 2007 R2 SP2 helps maintain consistency in system configuration and management. Rather than having each and every workstation, laptop, and server built from scratch in an ad hoc manner with configuration settings based on the individual desires of the IT professional building the system, SCCM uses templates in the build process.

The templates are created by the IT personnel to meet specific business, security, and functional application needs of the organization. Once a template is created, all systems of similar function can have the exact same template used to build and configure the system

with only the unique server name or other identifier being different from system to system. With the template-based installation, the organization can depend on consistency in build configuration for like servers, like desktops, and like laptops throughout the enterprise.

In fact, SCCM has additional components that ensure that the systems, once deployed, maintain the consistency by preventing users from updating systems using unsupported or unique update parameters. Rather, policies are established to update all systems of a similar functional role to be upgraded or updated the same. If a patch or update goes out to one system of a configuration type, then all systems of that configuration type are updated at the same (or relatively same) time. This concept, technically called Desired Configuration Management (DCM), can be audited and reports can be generated to show security officers and compliance auditors that standards are enforced throughout the data center and throughout workstation systems across an entire organization.

Major Features of System Center Configuration Manager

System Center Configuration Manager 2007 R2 SP2 has hundreds of features and functions that an IT administrator can leverage as part of their system configuration and management practices; some of the major features in the product are as follows:

- ▶ **Operating system deployment**—At the start of the system's life cycle is the installation of the core operating system. SCCM provides all the tools an organization needs to deploy an operating system, either as an imaged installation (formerly, organizations used Norton Ghost, but no longer need to because SCCM includes image creation and deployment tools) or as a scripted method of installation.
- ▶ **Patching and updating**—Once the operating system has been deployed, SCCM includes the mechanism to patch and update systems. Although many organizations use the Windows Server Update Services (WSUS), a free tool for patching and updating systems, SCCM leverages everything WSUS does but also provides IT administrators a more active patching and updating addition to WSUS. The Software Updates portion of the SCCM console, shown in Figure 1.2, is an example of the detail of the update information. The active update system enforces updates, forcing systems to be patched, updated, and rebooted based on policies that the IT department publishes and ensuring consistency in the update cycle of systems.
- ▶ **Asset tracking**—As part of the operating system deployment and patching and updating process, the management tool needs to know what type of hardware, software, and applications make up the system so the system can be properly updated. SCCM includes the tools necessary to track the hardware and software assets of the systems it is managing.
- ▶ **Remote control**—In the event that a user working on a system needs help, or that a system needs to be serviced, SCCM has a remote-control process that allows the IT administrator or a help desk individual to remotely control and support a user or manage a system whether the system is on the network or remote of the network.

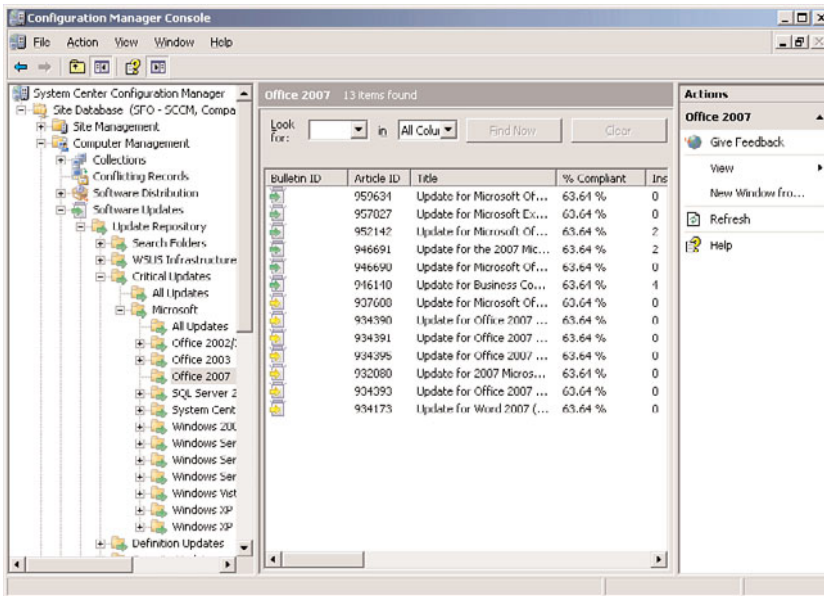


FIGURE 1.2 Details in the SCCM console relative to patching and updating systems.

- ▶ **Software deployment**—Although the operating system deployment will install the base operating system on a server or client system, applications need to be installed and managed as well. SCCM provides the tools to push out software applications, whether it is something as simple as a plug-in or utility or as complex as a complete suite or server-based application, including unique application configuration and customization.
- ▶ **Desired Configuration Management**—Beyond just having an operating system and applications installed on a system, keeping a system configured in a standard setup is crucial in consistency controls. SCCM provides a process called Desired Configuration Management, or DCM, that has policies established for system configurations so that a system cannot be changed or modified beyond the configuration standards set by policy for the system. This ensures all systems have the same software, drivers, updates, and configuration settings meeting stringent audit and controls standards consistent with regulatory compliance rules.
- ▶ **Internet Client**—A very significant component in SCCM is the Internet Client. In the past, for a system to be managed, the system had to be connected to the network. For remote and mobile systems, that means the system has to be VPN'd into the network to have patches and updates applied or for the IT department to inventory or remotely control the system. With the Internet Client and the use of a PKI certificate installed on the system, a remote or mobile system merely needs to be connected to the Internet anywhere in the world, and the SCCM client will automatically connect back to the corporate SCCM server through a secured tunnel to

allow SCCM to inventory, patch, apply policies, and update the system. The remote system does not need to VPN into the network or do anything other than simply establish connectivity to the Internet.

- **Reporting**—SCCM integrates into the product a report generation tool, shown in Figure 1.3, that comes with a full set of out-of-the-box reports, including the ability for IT personnel to create customized reports on everything from asset inventory reports to standard configuration reports to reports on the patch and update level of each laptop and desktop in the entire enterprise. Reports can also be customized in the report tool querying any data sets of information collected by SCCM and producing reports specific to the needs of the organization.

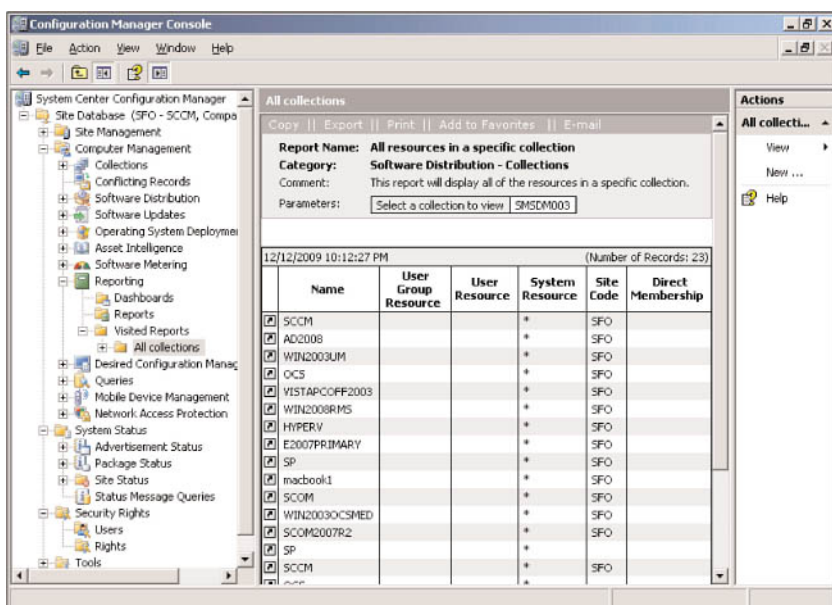


FIGURE 1.3 Reports tool built in to SCCM.

Background on System Center Configuration Manager

System Center Configuration Manager 2007 R2 SP2 is easily a half-dozen or more generations into the life cycle of the product. From its early roots as Systems Management Server, or SMS, that had a bad reputation for being a management product that took more to manage the management system than managing workstations and servers themselves, SCCM has come a long way.

Some of the major revisions and history of the product are as follows:

- **Systems Management Server v1.x**—Systems Management Server (SMS) v1.x had a few versions, 1.0, 1.1, and 1.2, all available in the mid-1990s to support systems typically in a Windows NT environment. Because Windows NT domains were clusters of

systems but not really a highly managed hierarchy of systems, SMS 1.x had its own site structure for identifying and managing systems. With most organizations at the time using Ghost to deploy system images, and patching and updating not really a common practice, SMS pretty much just provided the packaging of software programs and upgrades of software programs for systems. An expert who knew how to bundle up Microsoft Office or Adobe Acrobat into an MSI installation script had a full-time job as the process of packaging applications during these early days was neither easy nor intuitive. Smaller organizations found it was easier to just take a CD-ROM and walk from computer to computer to install software than try to create a “package” and hope that the package would deploy properly over the network.

- ▶ **Systems Management Server v2.0**—SMS 2.0 came out in 1999 and provided similar software-deployment processes as before; however, instead of using ad hoc site configurations, SMS 2.0 started to leverage subnets as its method of identifying systems on a network. SMS 2.0 also transitioned into the Active Directory era, although not without its challenges as it was a non-AD product that was somewhat set up to support an Active Directory environment. Needless to say, SMS 2.0 was about as successful as SMS 1.x was in helping in systems management.
- ▶ **Systems Management Server 2003 (also known as SMS v3.0)**—SMS 2003 came out to specifically support systems in an Active Directory environment, and although Microsoft now supported Active Directory sites, the product still required a packaging and scripting expert to be able to do anything with the product. Patching and updating became a requirement as viruses and worms spread across the Internet and a tool was needed to do the updates. So SMS 2003 was best known for its ability to provide patching and updating of systems; however, the setup and complexity of SMS 2003 to just control patching and updating allowed a number of other third-party companies like Alteris, Marimba, and LanDesk to challenge Microsoft in having an easier system for patching, updating, and deploying software.
- ▶ **System Center Configuration Manager 2007**—By 2007, Microsoft rebranded their management products under the System Center designation and finally broke away from the old legacy “site” concept of the Windows NT-based SMS product and fully redesigned the product for Active Directory, calling it System Center Configuration Manager 2007. With significantly better packaging, patching, and inventory tools along with a much better server role structure, SCCM 2007 finally “worked.” Organizations were now able to create software packages in minutes instead of days. Patching and updating leveraged the highly successful WSUS patching tool with enhancements added into the SCCM update for patching and updating to enforce updates, force system reboots, and better manage the mobile workforce.
- ▶ **System Center Configuration Manager 2007 SP1**—SCCM 2007 SP1 added support for managing Windows Vista systems as well as support for remote-management components that Intel built in to their chipset called vPro technologies. With systems with vPro built in, an SCCM administrator can wake up a powered-off system, boot the system to a remote-management guest operating system, and perform management tasks, including flashing the system BIOS without ever touching the actual system.

- ▶ **System Center Configuration Manager 2007 R2**—The R2 release of SCCM 2007 added automatic computer provisioning and multicast support for operating system deployments into the R2 release of the product. R2 also added App-V support in addition to ForeFront integration into the R2 release of the product.
- ▶ **System Center Configuration Manager 2007 R2 SP2**—Most recently, the release of SCCM 2007 R2 SP2 has now added the support of dozens of features, functions, and tools that support the imaging, management, and support of Windows 7 client systems.

What to Expect in the System Center Configuration Manager Chapters

In this book, four chapters are dedicated to the System Center Configuration Manager product. These chapters are as follows:

- ▶ **Chapter 2, “System Center Configuration Manager 2007 R2 Design and Planning”**—This chapter covers the architectural design, server placement, role placement, and planning of the deployment of System Center Configuration Manager 2007 R2 SP2 in the enterprise. The chapter addresses where to place site servers, discusses how to distribute images and large update files, introduces the various server roles and how the server roles can be placed all on a single server in a small environment or distributed to multiple servers, and covers the best practices that have been found in combining certain roles and the logic behind combining roles even in the largest of enterprises.
- ▶ **Chapter 3, “System Center Configuration Manager Implementation and Administration”**—Chapter 3 dives into the installation process of SCCM along with routine administrative tasks commonly used in managing an SCCM environment. This includes the familiarization of the SCCM management console features and how an administrator would use the management console to perform ongoing tasks.
- ▶ **Chapter 4, “Using Configuration Manager to Distribute Software, Updates, and Operating Systems”**—Chapter 4 gets into the meat of SCCM, focusing on core capabilities like distributing software, patching and updating, and creating and deploying operating systems. Any organization with SCCM implemented tends to use these features and functions at a minimum. The whole value in SCCM is to deploy operating systems (either imaged or scripted), patch and update systems, and deploy new software programs. This chapter covers the process as well as digs into tips, tricks, and lessons learned in sharing best practices used when deploying these features in the enterprise.
- ▶ **Chapter 5, “Configuration Manager Asset Management and Reporting”**—The final chapter on SCCM in this book covers other components, such as the asset management feature and the reporting capabilities built in to SCCM. Some organizations only use the asset feature in SCCM as the prerequisite to patch and update the system, whereas other organizations greatly utilize the asset management function for regulatory and compliance purposes. It’s the same with reporting: Some organizations never generate a report out of SCCM, just using SCCM for operating system deployment, updates, and software pushes. However, other organizations

heavily depend on the reporting capabilities in SCCM to generate reports for Sarbanes-Oxley (SOX) auditors or security compliance officers to prove the operational status of the systems.

System Center Configuration Manager 2007 R2 SP2 is a very powerful tool that is the start of the life cycle of a networked environment, providing templates and standard configurations for systems all the way through updates, management, and reporting. Jump to Chapters 2 through 5 of this book for specific information and deployment and configuration guidance on how SCCM can be best leveraged in your enterprise.

Understanding System Center Operations Manager

System Center Operations Manager (SCOM) 2007 R2 is the second product being addressed in this chapter. SCOM is used to monitor and alert network administrators when something (a server, workstation, network device, application, and so forth) is not working as expected, such as being offline, in a failed state, or even not running as fast as normal. The SCOM management console, shown in Figure 1.4, provides details about the events and errors of the systems being monitored and managed by SCOM.

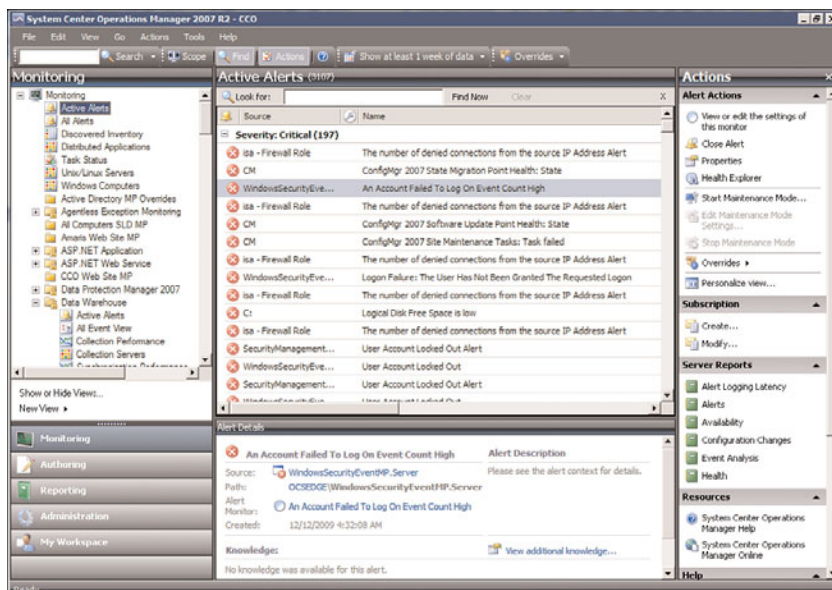


FIGURE 1.4 The System Center Operations Manager console.

In the past, system monitoring was simply monitoring and alerting when something was “down”; however, with System Center Operations Manager, the monitoring is proactive and alerts are triggered before problems cause a system to fail. SCOM proactively checks

the operation of systems and devices, and when the devices are performing differently than normal—which many times is a precursor to a pending system failure—SCOM begins the alert and notification process.

Business Solutions Addressed by System Center Operations Manager

System Center Operations Manager helps an organization be proactive about system operations rather than waiting for a server or application to fail, incur operational downtime, and recover from the failure. SCOM helps IT personnel ensure systems are running as expected. SCOM monitors the normal operation of servers, workstations, and applications to create a known baseline on how the systems are operating. When the systems fall out of the norm of the baseline, meaning that something is wrong, and while downtime has not occurred, the systems or applications are not running as they always do and IT personnel are then notified to review the situation and take corrective action.

SCOM also helps the IT department identify systems that should be replaced before others due to reliability issues. SCOM can keep track of system uptime and downtime and generate a report that ranks the reliability of systems based on their ongoing performance. If all things were equal in terms of age or depreciation schedule of systems, yet an organization will be replacing a portion of the systems, the reports can be used to identify which systems should be replaced first.

SCOM also has the ability to monitor applications as if a user is accessing the application and not just based on whether a system is operational or not. A system can appear to be fully operational, yet when users try to log on to the system, they could get logon errors or terrible access performance. SCOM has the ability to utilize automation by having a client system log on to a web server or an application server with stored credentials and validate that systems throughout the enterprise are more than operational and are serving users as expected.

SCOM can also be used to produce reports that help auditors and regulators validate that the organization's IT operations meet regulatory compliance requirements. Automated report generation for information such as password attempt violations, service-level agreement details, encrypted data access validation, and the like makes SCOM more than just a monitoring tool, but an information compliance reporting tool.

The bottom line is that SCOM helps IT personnel identify problems that need to be fixed before the problems create downtime that impacts the operations of the business. This is critical in keeping employees productive for internal servers, and helps an organization maintain business continuity when their servers host applications that help the organization generate revenues. A properly designed, implemented, and configured monitoring tool like SCOM can mean the difference of an organization focused on productivity and continuity versus an organization that is constantly recovering from system failures.

Major Features of System Center Operations Manager

System Center Operations Manager 2007 R2 has hundreds of features and functions that an IT administrator can leverage as part of their system monitoring and proactive management practices; some of the major features in the product are as follows:

- ▶ **Server and client system monitoring**—Key to SCOM is its ability to monitor servers and client systems. Using an agent that installs on the system (or agentless if the administrator desires), information about the system(s) is reported back to the SCOM monitoring server with operational data tracked and logged on a continuous basis.
- ▶ **Event correlation**—SCOM is smart enough to know that when a wide area network (WAN) connection is down, the status of all of the servers and devices on the other side of the WAN connection becomes unknown. Rather than sending hundreds of alerts that SCOM has lost contact with every device on the other side of a WAN, SCOM instead sends a single alert that the WAN connection is down and that the status of devices on the other side of the WAN are in an unknown state.
- ▶ **Event log collection**—Key to regulatory compliance reporting is to note system changes as well as potential security violations. SCOM has the ability to collect event logs and syslogs from systems, consolidate the data, and provide reports on the aggregate of information such as failed password attempts against all monitored servers in the environment.
- ▶ **System monitoring**—Monitoring in SCOM is more than just noting that a system is up or down, but also the general response time of the system and applications running on the system. Specific applications can be monitored using SCOM, such as monitoring SharePoint servers, SQL servers, or Exchange servers, as shown in Figure 1.5.
- ▶ **Client system monitoring**—Added in recent updates to SCOM is the ability to monitor and report on not just servers, but also client workstations in a network. Client system monitoring is commonly used to monitor and help manage and support critical client systems. A critical client system might be a laptop that belongs to a key executive, or it could be a workstation that serves as a print server or data collection device. Whatever the case, SCOM has the ability to monitor servers as well as client systems in the enterprise.
- ▶ **Application monitoring**—SCOM has the ability to monitor specific application and website URLs, not just to see if the servers are running or if the website is responding, but to actually confirm that the site is responding in a timely manner. This deep level of monitoring, shown in Figure 1.6, confirms response time and can even have test user accounts log on to session states to validate that a site or protected site is responding as expected.

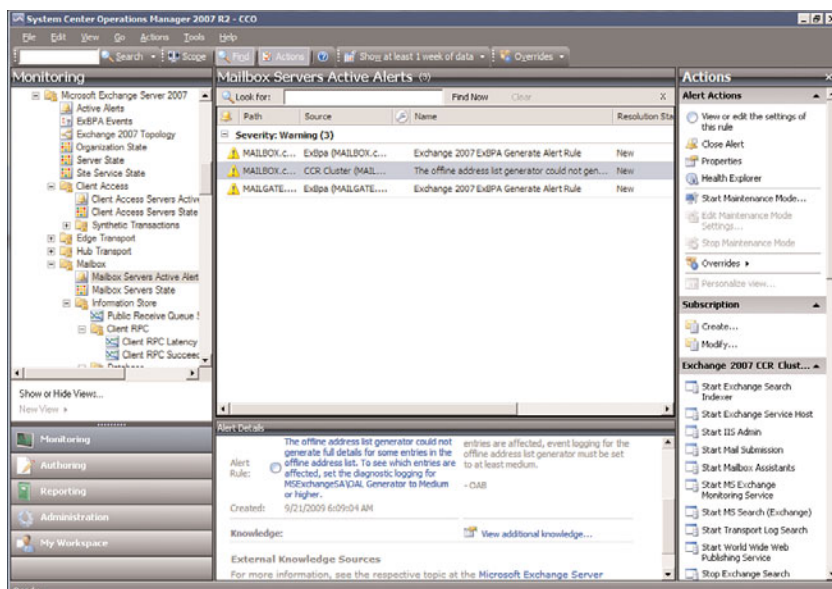


FIGURE 1.5 System monitoring and alerting in SCOM of specific servers in an environment.

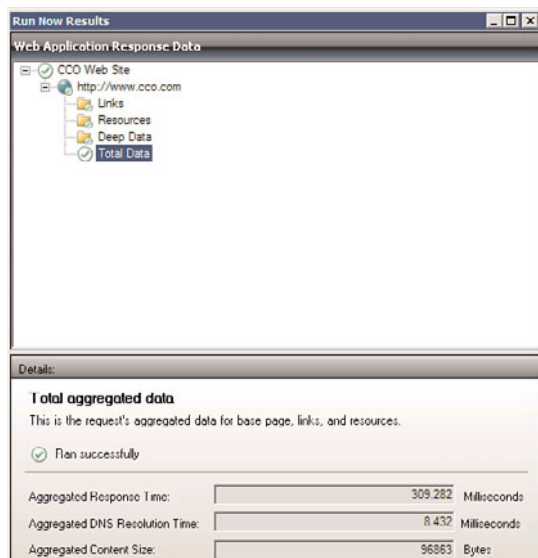


FIGURE 1.6 Monitoring applications and web URLs in SCOM.

- **Service-oriented management**—Traditional system monitoring treated all systems the same, so whether a single (only) system of its type in a network or a system that

has multiple redundant nodes, any system failure would result in a page or alert. SCOM is service oriented, meaning that if multiple servers exist for redundancy, the administrator will not be urgently paged or alerted if one of many systems is down. As long as the service (such as email routing, web hosting, or domain authentication) continues to operate, a different level of response (such as an email notification instead of an urgent page) is triggered.

- ▶ **Integrated solutions databases**—For administrators debugging a problem, the process usually involves grabbing event errors out of the log files, going to Microsoft TechNet to research the information, finding the solution, and then going back to the server to try the solution. With SCOM, it has Microsoft's TechNet information integrated into the system so that when an event occurs and shows up on the SCOM console, right there with the event error is the symptom information and recommended solution that an administrator would normally find in TechNet online. Additionally, SCOM not only has the information of what an administrator should do (like start and stop a service), but SCOM also presents a Restart Service option on the SCOM console screen for the administrator to simply click the option to restart the service. If that solution solves the problem, SCOM allows the administrator to choose to have that solution (like restarting the service) automatically run the next time the event occurs on ANY server in the environment. This self-healing process allows an organization to set processes that automatically trigger and resolve problems without having an administrator manually identify and perform a simple task.
- ▶ **Service-level agreement (SLA) tracking and reporting**—Many organizations have, publish, and manage to a specific service-level agreement metric, so if a network service is offline or degraded, the service-level quality is triggered and the overall service-level agreement is measured. SCOM has reports as well as a Dashboard view component that provides administrators the ability to know the status of system operations in the network.
- ▶ **Reporting**—With previous versions of SCOM, reporting was an external add-on. Effectively, if an administrator wanted a report on the status of systems, a separate report tool was run. With the latest releases of SCOM, the reports are available right within the SCOM console. From a common console, an administrator can monitor systems as well as generate reports on every managed system in the environment.

Background on System Center Operations Manager

System Center Operations Manager 2007 R2 has over a decade of history at Microsoft and many years before that before Microsoft acquired the technology back in 1999. From its early roots as Operations Manager 2000 to what is now System Center Operations Manager 2007 R2, SCOM has come a long way.

Some of the major revisions and history of the product are as follows:

- ▶ **NetIQ Enterprise Event Manager**—System Center Operations Manager has its roots from a 1999 product acquisition Microsoft made from NetIQ. The product, NetIQ

Enterprise Event Manager, was already a well-established tool for monitoring network environments and formed the basis of Microsoft's operations management offering.

- ▶ **Microsoft Operations Manager (MOM) 2000**—In 2000, Microsoft took the NetIQ product and rebranded it as Microsoft Operations Manager 2000, doing a little to include support for monitoring and managing the newly released Active Directory 2000 and Windows 2000 Server; however, for the most part, MOM 2000 was the NetIQ product with a new name. For the next five years, Microsoft released service packs and management packs to update the product to support all of the new Active Directory–supported products Microsoft was releasing like Exchange 2000 Server, Exchange Server 2003, SharePoint Portal Server 2001, SQL Server 2000, and the like.
- ▶ **Microsoft Operations Manager (MOM) 2005**—With the release of MOM 2005, Microsoft now had its first fully revised Microsoft monitoring and management product. Most organizations would consider this the Microsoft v2.0 of the product where core components such as event monitoring, event correlation, proactive monitoring, integration with TechNet support data, and the like made MOM 2005 a good Microsoft-focused monitoring and alerting product.
- ▶ **System Center Operations Manager 2007**—SCOM 2007 was a major improvement from Microsoft and one where the product was truly revised to meet the needs of enterprises. SCOM 2007 was now fully integrated with Active Directory so that servers and server roles (such as all Exchange front-end servers or all domain controllers) could be identified as a group. Role-based security was added so that there was better granular control over views and tasks that an administrator was able to perform. Also, the addition of an audit log collection system that auditors and regulators were looking for consolidated log information in which SCOM 2007 was able to extract log information and make that available for reporting.
- ▶ **System Center Operations Manager 2007 SP1**—SCOM 2007 SP1 included a rollup of all hotfixes for SCOM 2007, support for Windows 2008 as the base operating system that SCOM could run on, and a significant update to the Asset Intelligence (v1.5) component of SCOM for organizations that need better asset tracking and awareness.
- ▶ **System Center Operations Manager 2007 R2**—For those who have been using SCOM for a long time, the release of SCOM 2007 R2 was seen as a huge turning point of making SCOM a truly enterprise monitoring and management solution. SCOM 2007 R2 provided support for not only Windows-based servers and applications, but also now has support for non-Windows-based systems like UNIX and Linux system monitoring. SCOM 2007 R2 also has the ability of granularly defining Service Level Objectives, such as monitoring and assessing the response time of a specific logon procedure or web page view rather than simply pinging the system to see if it was up. In addition, significant improvements in scalability have been achieved, where monitoring of workloads can now be measured in the thousands of events per agent, allowing SCOM to reach into the largest data centers to manage Windows and non-Windows servers, network appliances and devices, and client systems throughout an enterprise.

What to Expect in the System Center Operations Manager Chapters

In this book, four chapters are dedicated to the System Center Operations Manager product. These chapters are as follows:

- ▶ **Chapter 6, “Operations Manager Design and Planning”**—This chapter covers the architectural design, server placement, role placement, and planning of the deployment of System Center Operations Manager 2007 R2 in the enterprise. The chapter addresses where to place management servers and where management packs fit in to SCOM for providing better data collection and reporting. This chapter also introduces the various server roles and how the server roles can be placed on a single server in a small environment or distributed to multiple servers, including best practices that have been found in combining certain roles and the logic behind combining roles even in the largest of enterprises.
- ▶ **Chapter 7, “Operations Manager Implementation and Administration”**—Chapter 7 dives into the installation process of SCOM along with routine administrative tasks commonly used in managing an SCOM environment. This includes the familiarization of the SCOM management console features and how an administrator would use the management console to perform ongoing tasks.
- ▶ **Chapter 8, “Using Operations Manager for Monitoring and Alerting”**—Chapter 8 gets into the meat of SCOM, focusing on core capabilities, such as monitoring individual servers and events and monitoring a collection of servers and creating event correlation to associate a series of servers, network devices, and applications for a better monitored view of key applications and network resources. Many organizations tend to just turn on the basic monitoring that SCOM has, which is good, but that’s not where the value is in SCOM. The value is creating automation tasks so that when an event occurs, SCOM can automatically assess the problem, correlate the problem to other events, and send the IT administrator a specific notification or alert that will help the administrator better manage the environment as a whole. This chapter covers the process as well as digs into tips, tricks, and lessons learned in sharing best practices of monitoring and alerting in the enterprise.
- ▶ **Chapter 9, “Using Operations Manager for Operations and Security Reporting”**—The final chapter on SCOM in this book covers the reporting capabilities built in to SCOM. In earlier versions of the Operations Manager product, Crystal Reports was used as an external reporting tool that reached into the MOM databases to generate reports, which was cumbersome and really more of an afterthought for reporting. With SCOM 2007 R2, reporting is done through SQL Reporting Services and integrated right into the main SCOM console. Rather than seeing reporting as something some people use occasionally, SCOM’s reporting takes management reports seriously as compliance officers, auditors, and executives want and need meaningful reports on the operations and management of their systems. SCOM 2007 R2 reporting provides out-of-the-box reports to track the most common business information reports needed out of the monitoring and security alerting system, with the ability

to customize reports specific to the needs of the organization. This chapter covers the out-of-the-box reports as well as how an administrator can customize reports specific to their needs.

System Center Operations Manager 2007 R2 is a very powerful tool that helps network administrators be proactive in the monitoring of their servers and network devices, both Microsoft and non-Microsoft, and have the ability to address problems before downtime occurs. Jump to Chapters 6 through 9 of this book for specific information and deployment and configuration guidance on how SCOM can be best leveraged in your enterprise.

Understanding System Center Data Protection Manager

System Center Data Protection Manager (DPM) 2010 is the recent update to the DPM 2007 product that was out for years. DPM 2010 backs up Windows-based servers in the environment, including domain controllers, Exchange servers, SharePoint servers, file servers, SQL servers, and Windows workstations. Unlike traditional backup systems that kicked off in the middle of the night to “stream” the entire content of a server to tape, DPM backs up servers incrementally all day long and, in fact, does incremental backups of critical servers like Exchange or SharePoint every 15 minutes. Because the data backups are now done incrementally throughout the day, the load on the servers is minimal and the data is no more than a few minutes behind.

At any time, the administrator can reach into a backup from just a few minutes ago and initiate a restore of the data. Additionally, components within DPM 2010 allow the end user to restore information themselves in what is called self-service recovery. As an example, if a user is working off a file share in Windows (XP SP2 or higher) and accidentally deletes or overwrites a file, that user can simply right-click the file share, choose Previous Versions, and see previous versions of the file that was deleted or overwritten and choose to self-recover the file immediately.

Also, because DPM does not use tape as the primary medium but rather hard disk storage, the recovery of data, whether it is 15 minutes old, 15 days old, or even 15 weeks old, is done in seconds. Digital data backups as a primary method of backup and recovery provide faster backup and restore times, and DPM data can secondarily be written to tape or replicated across a WAN or the Internet to be stored offsite. Third-party providers can provide DPM secondary storage “in the cloud” so that an organization can bypass tape altogether and just push critical backups to an external third-party provider for safe recovery over the Internet in the event of a local site failure.

System Center Data Protection Manager 2010 provides the ability for protection groups to be created, as shown in Figure 1.7, where file servers, Exchange servers, SharePoint servers, SQL servers, or the like have varying backup schedules to ensure the successful backup of the application in a manner specific to the application.

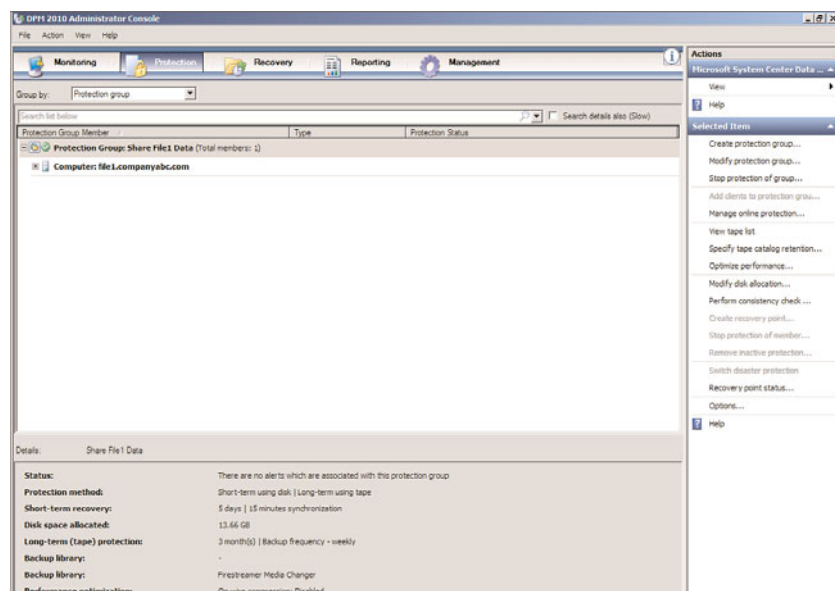


FIGURE 1.7 The System Center Data Protection Manager 2010 console.

Business Solutions Addressed by System Center Data Protection Manager

For most organizations, *backup* has traditionally been something that is done every night as a “set-it-and-forget-it” process as insurance that if a server catastrophically fails, the administrator can go back to a tape and perform a recovery. Unfortunately, because *backup* has been seen as a necessity to take tapes offsite, but not a serious method of actual recovery, most organizations who have had to go back to tape have found that the data on the tape was either not accessible (due to tape corruption) or not complete (organization was only backing up one component of a server, not all data components). DPM provides a “set-it-and-forget-it” medium for backup that is more reliable than the traditional method in that the medium is digital hard disk data, not flimsy electromagnetic tape. In addition, DPM has the intelligence of backing up not only “the server,” but also backing up databases and logs together, or System State and databases together that are necessary for a successful recovery.

However, for organizations that want more than just data backed up, DPM is a component of a disaster recovery and actual business continuity strategy. By incrementally backing up data to DPM and then replicating the DPM data to other sites in real time, an organization has effectively created a process for full data recovery in a separate site. The same backup process in DPM that provides full recovery in the once-every-30-year type of

scenario can be used from day to day by users themselves to self-recover deleted documents or email messages.

DPM takes an age-old process of full backups and provides day-to-day value to users to perform a simple recovery task of their own data all the way through the recovery of an entire data center in the event of a catastrophic failure.

Major Features of System Center Data Protection Manager

The System Center Data Protection Manager 2010 product has a wealth of features and functions that help an IT administrator back up, protect, and incrementally recover data on servers throughout the organization; some of the specific major features in the product are as follows:

- ▶ **Back up Microsoft-based servers**—As a Microsoft backup product, DPM knows how to back up Microsoft products in a manner that Microsoft wants their applications like Exchange, SQL, or SharePoint to be backed up. DPM knows that a successful SharePoint restoral requires a clean backup of the System State, Configuration Database, and Content Database at a specific snapshot point in time and, thus, when DPM backs up SharePoint, it backs up all of the necessary files and information. DPM has the ability to back up Active Directory, Windows servers, Windows file systems, Exchange servers, SharePoint servers, SQL servers, and Windows client systems.

NOTE

The biggest complaint about DPM is that although it does back up Microsoft products really, really well, it has no facility to back up non-Microsoft products today. For organizations that want to back up their Oracle databases, their Linux servers, or the like, the organization needs another backup product at this time. Choosing DPM as a backup product for an organization that is exclusively Microsoft-based is an easy decision. For mixed environments, many organizations still choose DPM to back up their Microsoft products as it is the best-of-breed solution in backing up (and, more important, recovering) Microsoft servers and applications.

- ▶ **Back up file server data with self-service user recovery**—DPM has the ability to back up file servers, including file permissions on the files on the system. With DPM file backup implemented, end users can self-service recover files that have been accidentally deleted or even overwritten with versions of files that have been backed up and are stored on the DPM 2010 server. This self-service function leverages the “previous versions” capability in Windows, as shown in Figure 1.8.
- ▶ **Back up Microsoft Exchange databases**—DPM also has built-in intelligence to back up Exchange servers, including Exchange Server 2003, Exchange Server 2007, and Exchange Server 2010, and not just the databases but also the log files and associated information necessary to allow for a successful recovery of a single Exchange database or an entire Exchange server. Additionally, DPM can back up a passive node

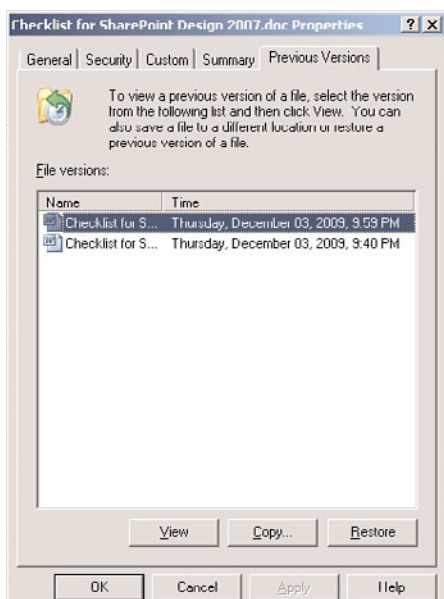


FIGURE 1.8 Self-service recovery of files leveraging DPM.

of an Exchange cluster, or in Exchange 2010, DPM can back up a replica copy of the Exchange data (not the primary active database), thus allowing a backup to proceed in the middle of the day with absolutely no impact on users. The recovery process of Exchange leverages the recovery storage group/recovery database concept in Exchange, where the data can automatically be recovered to a live running Exchange server that then allows the administrator to mount the database and selectively recover a single mailbox or even a single mail message directly into a user's mailbox.

- **Back up SharePoint data, including recovery straight to the source data location**—As mentioned as an example in the Windows Server backup bullet, DPM is intelligent enough to know to back up all components of a SharePoint environment for the ability to successfully restore the SharePoint server. DPM can back up SharePoint 2007 and SharePoint 2010 with the added benefit of SharePoint 2010 backups that it can do a restoral directly to a live working SharePoint 2010 server. This is more a feature of SharePoint 2010 that allows for the recovery straight to a running SharePoint 2010 production server that did not exist in SharePoint 2007. SharePoint 2007 requires data to be restored to a replica of the SharePoint 2007 production environment and then data extracted from that replica farm and inserted into the production SharePoint 2007 environment. SharePoint 2010 can have data restored right into a production document library or list, or even the full recovery of a site. DPM 2010 has the ability of facilitating the successful recovery process into a live SharePoint 2010 environment.

- **Back up SQL data, including automatic backup of databases added to the SQL server**—DPM 2010 can back up and recover SQL servers in a production environment. DPM 2010 backups of SQL servers not only allow for the backup of a specific targeted server, but an option can be triggered so that when additional databases or instances are added to a server, DPM automatically adds those additions to the backup group. In the past, if an administrator did not update their tape backup software to specifically back up a new database, the new database would never be backed up. DPM can be set to dynamically back up new databases added to a server. Additionally, once data has been backed up using DPM, the administrator can go into the Recovery tab of the DPM 2010 console and choose files, documents, databases, or entire servers from any specific backup and initiate a restore of the information. The information from the recovery page of the console is shown in Figure 1.9.

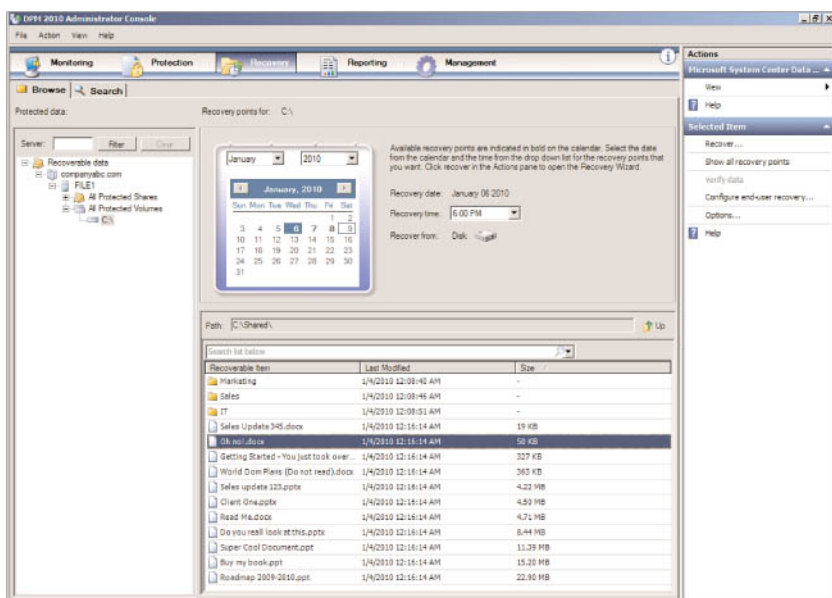


FIGURE 1.9 Recovery page from the DPM 2010 console.

- **Backup of Hyper-V physical servers, including direct VHD recovery**—DPM 2010 has the ability to back up Hyper-V host servers, including the ability to selectively recover a specific Hyper-V guest session from that server-based backup. This provides an administrator the ability to target a server or series of Hyper-V host servers and then selectively choose to recover specific guest session instances.
- **Long-term storage of data to tape**—Although DPM provides the initial backup of information digitally to hard disk media, data on the DPM server can then secondarily be written to tape for long-term storage. Data written to tape can be used to recover a single backup instance or can be used to recover an entire DPM server itself.

- **Long-term storage of data pushed to the cloud**—Lastly, DPM 2010 data can be replicated offsite, whether that is replicating data to another DPM server in another organization-owned or managed data center, or replicating the DPM data to a third-party hosted storage provider. By replicating DPM data offsite over a WAN or Internet connection, an organization might not even need to ever have tapes or manage tapes again.



Background on System Center Data Protection Manager

System Center Data Protection Manager 2010 has gone through several revisions in just the past three to four years at Microsoft. Microsoft has done a good job updating the product to support more and more of what organizations want in a backup and recovery product. Each successive update of DPM has brought along major feature improvements; some of the major revisions and history of the product are as follows:

- **Data Protection Manager 2006**—DPM was released in 2005 as DPM 2006 and provided the backup of basic Windows Active Directory and file servers. Because it only backed up file servers and not critical business applications like Exchange or SQL, DPM 2006 did not have a lot of organizations jump on and adopt the product.
- **Data Protection Manager 2007**—At the end of 2007, Microsoft shipped DPM 2007 that finally supported the backup and recovery of Exchange Server 2003, Exchange Server 2007, SQL Server 2000, and SQL Server 2005. This was significant as DPM could now be used to back up real applications in the enterprise.
- **Data Protection Manager 2007 SP1**—Early in 2009, Microsoft released SP1 of DPM 2007 that provided full support for backing up Exchange Server 2007 Cluster Continuous Replication (CCR) clusters, Microsoft Office SharePoint Server 2007 servers with intelligent backup and recovery of entire SharePoint states, support for backing up Hyper-V virtualized environments, and the ability to back up to the cloud with initial companies like Iron Mountain providing host offsite cloud services.
- **Data Protection Manager 2010**—Most recently, the release of DPM 2010 provided the backup of entire Hyper-V Live Migration and Cluster Share Volume (CSV) backups and recoveries, backup of Windows client systems, and the ability to back up the latest Exchange Server 2010 and Microsoft Office SharePoint Server 2010 environments.

What to Expect in the System Center Data Protection Manager Chapters

In this book, two chapters are dedicated to the System Center Data Protection Manager product. These chapters are as follows:

- **Chapter 10, “Data Protection Manager 2010 Design, Planning, Implementation, and Administration”**—This chapter covers the architectural design, server sizing, server placement, and planning of the deployment of System Center Data Protection

Manager 2010 in the enterprise. The chapter provides modeling information on how much hard disk storage is needed to back up servers as well as best practices on the retention period of data (whether data should be backed up every 15 minutes, every hour, or every day and whether data should be stored for three days, a week, a month, or a year).

- **Chapter 11, “Using Data Protection Manager 2010 to Protect File Systems, Exchange, SQL, and SharePoint”**—This chapter provides information on how an administrator would use DPM 2010 to specifically protect and recover key applications and workloads such as file systems, Exchange, SQL, and SharePoint.

System Center Data Protection Manager 2010 with its support for doing 15-minute incremental backups of key business applications along with the ability to have self-service of information by end users themselves has vaulted DPM as a valuable tool for an organization to have in its business continuity and data-recovery strategy. Jump to Chapters 10 and 11 of this book for specific information and deployment and configuration guidance on how DPM can be best leveraged in your enterprise.

Understanding System Center Virtual Machine Manager

In the past two to three years, server virtualization has shifted from something that organizations used to do in their test and development environments to something where organizations have 50% or more of their production servers virtualized. Microsoft’s System Center Virtual Machine Manager (VMM) 2008 R2 provides a number of very valuable tools for an organization with both Microsoft Hyper-V virtual servers as well as VMware virtual servers to better manage and support their virtualized environment.

VMM, like DPM, is a relative newcomer to the Microsoft management suite of products; however, just like how VMware dominated the virtualization marketplace in 2007 as the de facto standard, in just a couple of short years, Microsoft released two significant products and updates that now Hyper-V has thrust into being one of the major players in virtualization. The key to the growth of virtualization came from the release of x64-bit systems along with vendor support for virtualization.

With 32-bit systems and a limitation of 4GB of RAM in a server, there weren’t many ways you could split 4GB of RAM and host production server workloads. At most, maybe an organization could get two to three small applications to run on a single virtual host system. However with 16GB, 32GB, even 64GB being common in servers with 8-core or 16-core CPUs in a single host server, a single system can easily be split 5 ways, 10 ways, or even 15 ways, providing a significant density of virtual guest sessions in a single hosted server system.

With that many guest sessions running on a single server, organizations need a way to best manage the environment. VMM 2008 R2 provides the tools to migrate physical servers into a Hyper-V guest session, and from a single console view, shown in Figure 1.10, administrators can view and manage all of the virtual host servers and guest sessions from a single console interface.

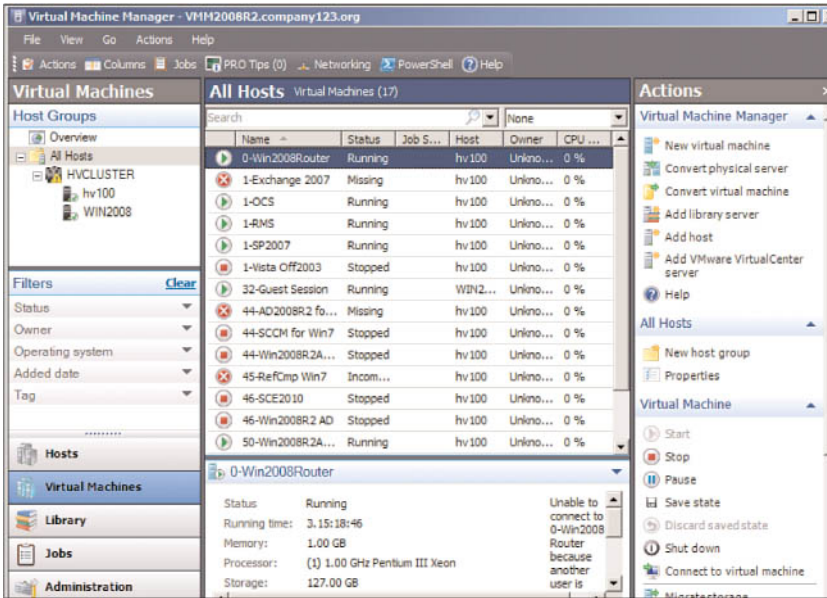


FIGURE 1.10 System Center Virtual Machine Manager console.

Business Solutions Addressed by System Center Virtual Machine Manager

The business value that VMM 2008 R2 provides is the ability for the IT administrator to centrally manage their host servers and guest session, regardless of whether the systems are Microsoft Hyper-V or VMware ESX hosts from a single console. With the proliferation of virtual hosts, VMM provides the needed tool to manage the guest sessions with standard builds, allocate the proper amount of memory and processing capacity, balance the workload of guest sessions across host servers, and ultimately maintain uptime of host servers in an environment.

As organizations take advantage of server consolidation by getting rid of physical servers and creating significantly fewer virtual host systems, the need to migrate physical workloads into virtualized workloads quickly and easily becomes an important task. VMM 2008 R2 can capture physical systems and migrate them to virtual guest sessions as well as migrate other virtualized guest sessions (running on Microsoft Virtual Server 2005 or on VMware) and migrate them to the latest Hyper-V host environment.

Organizations have migrated hundreds of physical servers to just a handful of physical host servers saving the organization hundreds of thousands of dollars on hardware maintenance contracts, electrical power, physical server rack space, and physical host server support costs.

Major Features of System Center Virtual Machine Manager

System Center Virtual Machine Manager has a whole list of features and functions that help an IT administrator manage virtual host servers as well as virtual guest sessions; some of the major features in the product are as follows:

- ▶ **Single view of all virtual host systems (Hyper-V and VMware)**—At the root of the Virtual Machine Manager product is its ability to consolidate into a single console view all Microsoft Hyper-V and VMware host servers and guest sessions running in the environment.
- ▶ **Ability to perform physical-to-virtual (P2V) conversions**—Once the centralized monitoring console is available, servers can be easily migrated from physical systems to virtual systems in what is called a P2V migration process.
- ▶ **Ability to perform virtual-to-virtual (V2V) conversions**—For systems that are already running on a different, possibly older virtualization platform like Microsoft Virtual Server 2005 or VMware, the virtual-to-virtual (V2V) feature in VMM 2008 converts the virtual guest sessions into the latest Microsoft Hyper-V virtual guest session standard.
- ▶ **Delegate the administration and management of virtual guest sessions to other administrators**—For larger enterprises where certain administrators are in charge of all of their servers, instead of having, for example, 10 physical servers in a rack that an Exchange or SQL administrator would be in charge of, the administrator might find their servers spread across several shared Hyper-V physical host servers. Rather than giving an administrator access to all of the guest sessions running on all of the host servers, VMM 2008 R2 provides an administrator the ability to group together servers and delegate the administration of those virtual guest server sessions to other administrators. Therefore, an Exchange administrator will be able to see, administer, and manage the Exchange servers regardless of which physical host server the guest sessions are running on. And likely, the SQL administrator or the SharePoint administrator will be able to see their servers in a centralized view without having access to servers that they should not have access to.
- ▶ **Self-service creation of guest sessions from templates**—As much as the administration of guest sessions can be delegated to various administrators, when those administrators (or others in the organization) need to create a new guest session, the ability to delegate the creation of guest sessions is a core component of the VMM 2008 R2 product. An administrator can delegate guest session creation to other users, nonadministrators, using the self-service portal web console, shown in Figure 1.11, that is part of the Virtual Machine Manager 2008 R2 product. A self-service user is given a set amount of resources like 8GB of RAM and four core processors to use as

they want. They can create a single guest session using all 8GB and four cores, or the user can create four guest sessions running 2GB and a single core each, or any variation of resource allocation. This provides administrators the ability to share Hyper-V host resources without having to give a user full access to create as many guest sessions as they want and impact the overall performance of the host servers in the environment.

- **Manage both Hyper-V and VMware guest sessions**—Finally, as mentioned previously, VMM 2008 R2 can connect to a VMware Vi3 environment as well as directly manage VMware ESX servers, and as such can help an administrator in a mixed environment to manage and support virtual servers from both Microsoft and from VMware from a single console.

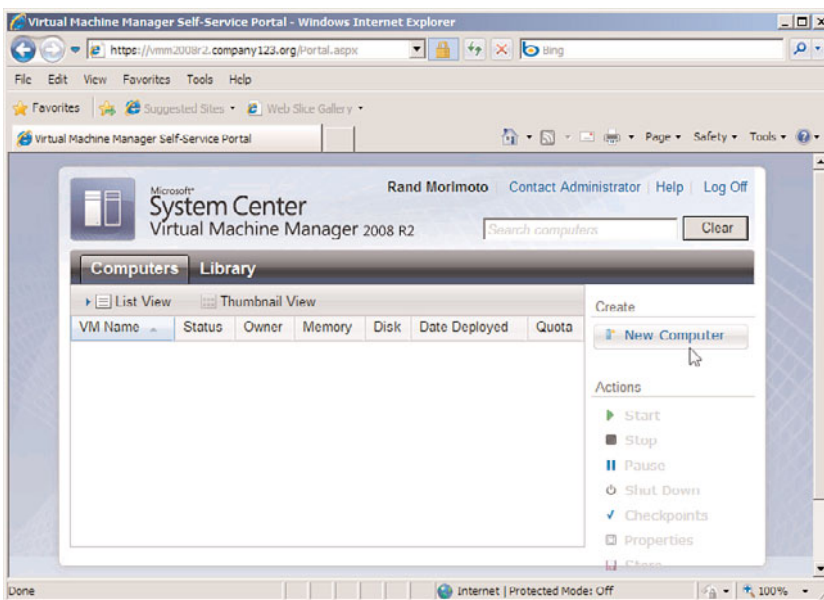


FIGURE 1.11 Self-service creation of guest sessions in VMM.

Background on System Center Virtual Machine Manager

System Center Virtual Machine Manager is a relative newcomer to the System Center family of products. From the first version coming out in 2007 to support Microsoft's late entry into the server virtualization space to the current version of Virtual Machine Manager 2008 R2, Microsoft has made significant headway in advancing the virtualization support and features and functions of the product.

Some of the major revisions and history of the product are as follows:

- ▶ **Virtual Machine Manager 2007 (VMM 2007)**—Virtual Machine Manager 2007 entered the market to support virtual guest sessions running on Microsoft Virtual Server 2005. All of the current technologies like P2V, V2V, and delegated administration existed in the VMM 2007 product; however, because Virtual Server 2005 only supported 32-bit guest sessions and not 64-bit guest sessions, very few organizations adopted Virtual Server 2005 and, thus, VMM 2007 did not have a significant following.
- ▶ **Virtual Machine Manager 2008 (VMM 2008)**—With the release of Hyper-V in Windows Server 2008 along with the support for 64-bit hosts and guest sessions, now organizations had the ability of getting 5, 10, or 15 guest sessions on a single host server, and the ability to manage that many guest sessions suggested that a management tool was necessary. VMM 2008 was updated to support Hyper-V and as organizations started to deploy Hyper-V, more organizations started to install and use VMM 2008.
- ▶ **Virtual Machine Manager 2008 (VMM 2008 R2)**—In less than a year, Microsoft updated Hyper-V with the release of Windows Server 2008 R2 so that Hyper-V R2 supported “live migration” failover between host servers. Hyper-V R2 was now seen as enterprise ready and organizations started to adopt Hyper-V R2 as their server virtualization platform. At the same time, Microsoft released VMM 2008 R2 to support the added capabilities found in Hyper-V R2.

What to Expect in the System Center Virtual Machine Manager Chapters

In this book, two chapters are dedicated to the System Center Virtual Machine Manager product. These chapters are as follows:

- ▶ **Chapter 12, “Virtual Machine Manager 2008 R2 Design, Planning, and Implementation”**—This chapter covers the architectural design, planning, and rollout of VMM 2008 R2 in the enterprise. Concepts such as console servers, self-service portal servers, and management servers are defined with best practices shared on how to properly set up, configure, and tune VMM 2008 R2.
- ▶ **Chapter 13, “Managing a Hyper-V Environment with Virtual Machine Manager 2008 R2”**—This chapter covers the management and administration tasks in VMM. Performing tasks like delegated administration and self-service portals is covered and addressed in this chapter.

System Center Virtual Machine Manager 2008 R2 even just for the P2V and V2V capabilities is of great value to organizations—let alone the ability for administrators to see all virtual servers in their environment along with the ability to delegate administration to others in the organization. Jump to Chapters 12 and 13 of this book for specific information and deployment and configuration guidance on how VMM can be best leveraged in your enterprise.

Understanding System Center Service Manager

System Center Service Manager (SCSM) 2010 is a long-awaited addition to the System Center family. SCSM 2010 is over five years in the making—something Microsoft built as an entire tool and released as a beta only to be pulled back, completely redone, and rereleased as a completely new and improved product. SCSM 2010 is a help desk and change-control management tool that rolls up information collected in other System Center products and provides IT staff the ability to track, manage, and report on information from all of the various System Center components. The System Center Service Manager 2010 console, shown in Figure 1.12, is the focal point of the key management capabilities built in to SCSM.

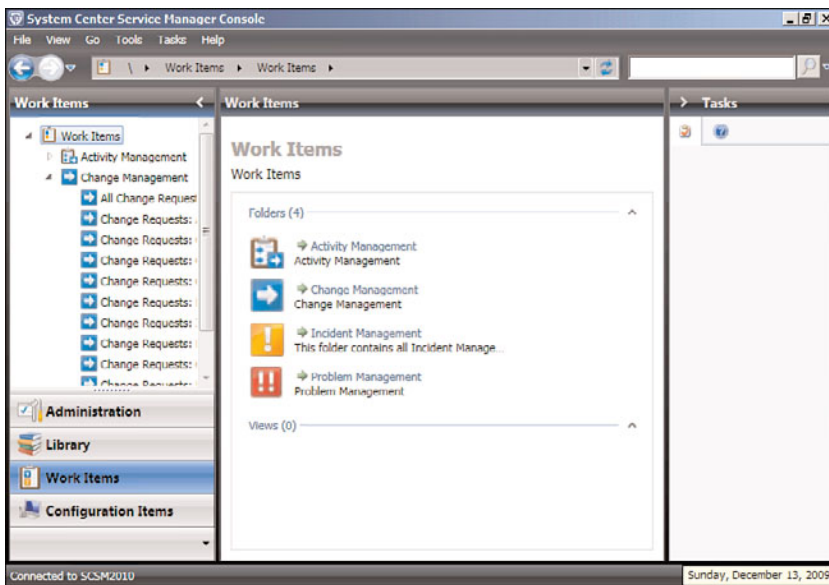


FIGURE 1.12 System Center Service Manager console.

Business Solutions Addressed by System Center Service Manager

System Center Service Manager 2010 consolidates reports from client, server, physical, and virtual environments into a single reporting repository. SCSM allows an organization to leverage its investment in one System Center product into other System Center products. With the need to have formalized structure in change management, incident management, and reporting, SCSM leverages ITIL practices and procedures for an organization. Even being ITIL based, organizations that don't have a formal management practice can begin developing one based on the built-in processes in SCSM 2010.

Also important to organizations is managing and maintaining change-control processes so that network administrators don't patch or update systems in the middle of the day and

accidentally bring down servers in the process. Or, as updates are needed on servers, rather than doing them one at a time, a maintenance window can be created where all updates are applied to a system at the same time. This managed change-control and maintenance process is something that SCSM 2010 helps to maintain and manage.

SCSM 2010 improves the integration between existing investments in System Center products, including inventory information, error reports, reporting details, and the like rolled up to SCSM for centralized information access and report generation.

Major Features of System Center Service Manager

System Center Service Manager is a very extensive product covering information reporting and management; some of the major features in the product are as follows:

- ▶ **Incident management**—Incident management is probably better known as a “help desk”; however, beyond just taking in problem reports and processing the problem reports from users, SCSM ties into the System Center Operations Manager product so that errors and events coming off servers and workstations automatically trigger incident events in SCSM. Additionally, users can submit problem tickets or incidents whether through a console screen or by submitting the request via email or even text message that enters the incident management system where help desk or IT staff can provide support and assistance. The incident management system in SCSM, as shown in Figure 1.13, provides the ability to have problems or incidents easily submitted to the organization’s IT support personnel.
- ▶ **Change control**—Built in to SCSM 2010 is a change-control monitoring and management system. Change control leverages a workflow process where a change request is submitted, and a workflow routes the change request to key personnel who need to review and approve the change to be performed. Beyond just a workflow approval process, SCSM 2010 tracks that change control, logs the change, monitors and manages the change, and keeps a running record of the change so that if problems occur in the future on the system, the information about all historical updates and changes are tracked and available for the administrators to see.
- ▶ **Consolidated reporting**—SCSM 2010 collects information from other Microsoft System Center products as well as creates connectors and links to the databases in other System Center products for consolidated reporting. Rather than having each individual database store isolated information, data from multiple sources can be viewed and analyzed to help make decisions about the operation, maintenance, and support of the environment.
- ▶ **Self-service access**—Rather than simply a help desk submission system, the self-service access feature in SCSM 2010 allows a user to search the knowledge base to see if anyone else in the organization has had the same problem and, if so, what the fix was to the problem. Many users would rather fix a problem themselves if the fix is

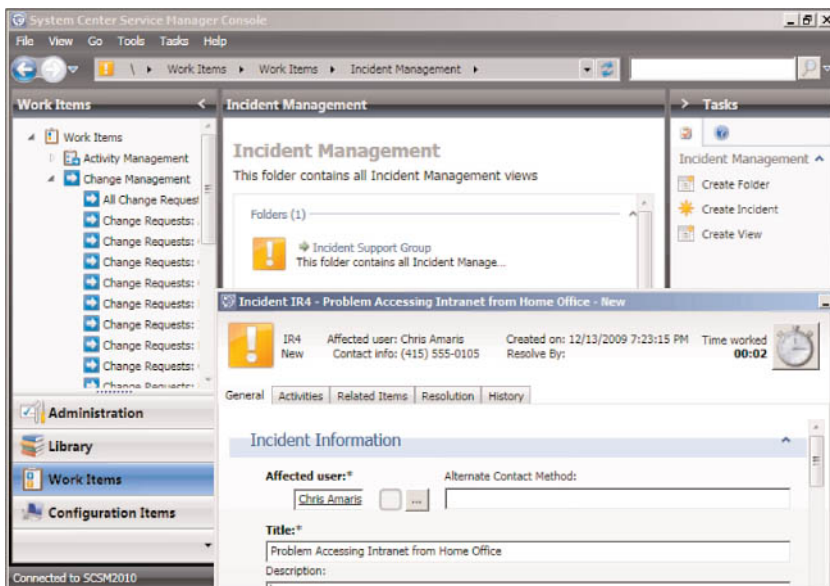


FIGURE 1.13 Incident management within SCSM.

known and works, and as such, SCSM tracks the problem tickets and solutions of previous fixes on systems and databases. The problems and solutions can be queried by the IT staff or by end users to share the knowledge and experiences of previous service requests.

Background on System Center Service Manager

System Center Service Manager 2010 is the first version of this product released to the public; however, internally, this product has been five years in the making. The product effectively had its version 1.0 release several years ago as a SharePoint-based tool, which was called System Center Service Desk at the time that Microsoft released it in beta to a limited number of organizations. Although the feedback was very positive on the feature sets, because it was based on SharePoint (2003 at the time), the product did not fit into the mold of other System Center products at the time, such as the robust management consoles found in System Center Configuration Manager or Operations Manager.

Microsoft went back to the drawing board and released a new version of System Center Service Manager, this time with the same management interface found in other System Center products. This release, probably dubbed v2.0 of the product, was limited to just help desk-type incident management and reporting at a time when all other management

tools in the industry had evolved to support more than just trouble tickets, but to really address fully formed ITIL-based change-control and incident management systems.

Not ready yet for release, Microsoft spent another couple of years adding more functions to the Service Manager product to get it at par with what other service management tools on the marketplace included. With the release of System Center Service Manager 2010, the product is probably like a v3.0 or v4.0 of the product, with years of development, redevelopment, and updates before its formal debut.

What to Expect in the System Center Service Manager Chapters

In this book, three chapters are dedicated to the System Center Service Manager 2010 product. These chapters are as follows:

- ▶ **Chapter 14, “Service Manager 2010 Design, Planning, and Implementation”**—This chapter covers the architectural design, server placement, and planning of the deployment of System Center Service Manager 2010 in the enterprise. The chapter addresses where to place management console servers as well as self-service portals for users to access, submit, and get responses back from the SCSM system. This chapter also covers the integration of SCSM 2010 into other System Center products as well as the integration of SCSM into Active Directory.
- ▶ **Chapter 15, “Using Service Manager 2010 for Incident Tracking and Help Desk Support”**—Chapter 15 drills down into incident tracking and help desk support features in SCSM 2010 on how to configure the tracking system as well as how IT personnel and users interact with the tracking and incident management system. This chapter also covers the self-service features and capabilities built in to System Center Service Manager 2010.
- ▶ **Chapter 16, “Using Service Manager 2010 Change-Control Management”**—Chapter 16 details the change management control process where information comes in from System Center Operations Manager as well as from users and administrators to be managed and processed. This includes the workflow process, the integration of the workflow into day-to-day systems management, and the scheduled maintenance and update process key to a managed change-control system.

System Center Service Manager 2010 brings together the various System Center products into a single tool that helps IT organizations manage problems or incidents in their environment. Jump to Chapters 14 through 16 of this book for specific information and deployment and configuration guidance on how SCSM can be best leveraged in your enterprise.

Understanding System Center Capacity Planner

Not formally included in the licensing of the System Center suite, System Center Capacity Planner 2007 is a tool that helps organizations run models for determining the size and system requirements for products like Microsoft Exchange and others. By entering the number of users, the amount of messages sent and received, the number of sites, and the workload of communications traffic, SCCP helps IT architects and designers map out a design and plan for servers to host applications in their environment.

The System Center Capacity Planner 2007 main screen, shown in Figure 1.14, provides the main console for launching capacity assessments.

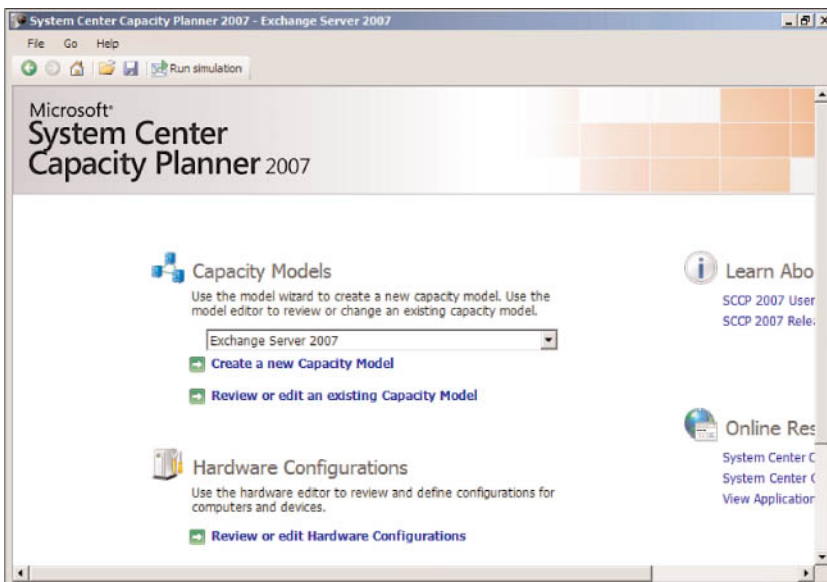


FIGURE 1.14 System Center Capacity Planner main screen.

Business Solutions Addressed by System Center Capacity Planner

System Center Capacity Planner is used to proactively (rather than reactively) size and scale servers for applications. Rather than building out servers based on a guess and then having to add more RAM, disk space, or CPU to the configuration to support the number of users or the amount of traffic/system demand of the users, Capacity Planner 2007 generates a model that suggests the type of system configurations and network bandwidth utilization anticipated in a system rollout.

Even for organizations that have already rolled out something like Exchange Server 2007 that might be facing sluggish performance or users complaining they are getting response-time errors, a model can be run based on actual user data to determine what SCCP suggests the servers should have in terms of performance and capacity.

SCCP can be used either proactively during the planning process or reactively after performance problems are experienced to determine what might be appropriate for an environment in terms of system configuration.

Major Features of System Center Capacity Planner

The System Center Capacity Planner tool has a number of built-in features and functions for performance and capacity modeling; some of the major features in the product are as follows:

- **Performance assessment modeling**—System Center Capacity Planner 2007 allows for information about an environment to be input into the system with a model simulation to be run to confirm the anticipated performance of the configuration. In the System Center Capacity Planner tool, simulation results are generated and displayed in a report similar to the one shown in Figure 1.15.

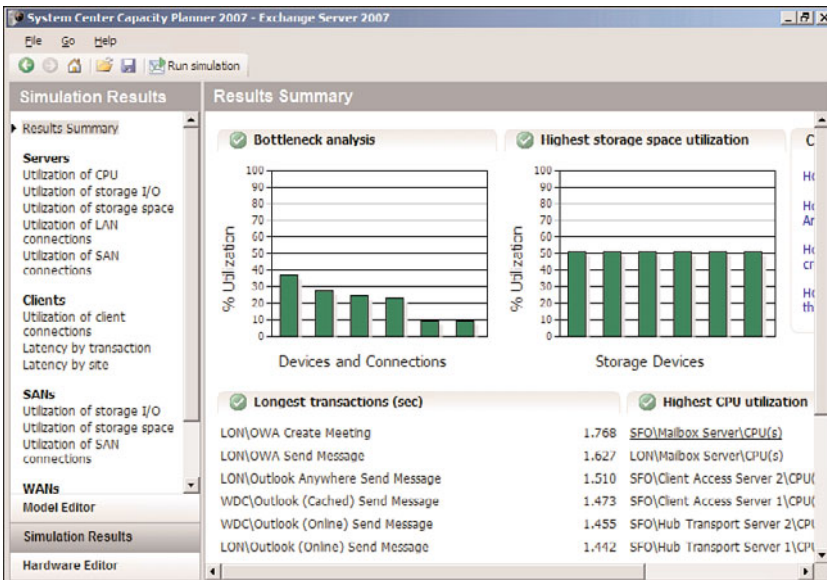


FIGURE 1.15 Simulation results report out of System Center Capacity Planner 2007.

- **Capacity analysis**—SCCP can also be used to perform a capacity analysis to determine peak performance demands as well as maximum capacity of a specifically configured environment. This is helpful for organizations that are growing quickly and want to determine the maximum number of users or the maximum size mailboxes that the environment can realistically support. This peak load and maximum

capacity analysis can be used to determine the suitability of adding an additional server or adding more memory or processing performance to an existing system to see the results of the configuration.

- ▶ **Current usage analysis**—Another angle to performing capacity analysis is to enter in the current usage of the environment and determine what percentage of workload the current usage is placing on the existing environment. Are the servers running at 25% of capacity or 75% of capacity given the current workload and configuration? This helps an organization ensure that the servers in place are configured to meet the current and near-terms demands of the organization.
- ▶ **Reporting and recommendations**—The end result of SCCP is the reports it generates. Reports are generated that provide an analysis of the capacity usage and demands of the environment. These reports can be used to determine what type of hardware needs to be purchased or can be used for budgetary purposes to project what hardware will be needed over the upcoming year to keep up with the operating demands of the organization.

T

Background on System Center Capacity Planner

System Center Capacity Planner has been available as a download for the past several years, initially as a basic Windows Server capacity analyzer and modeling tool, and more recently with additional components added to the product that enhanced the modeling capabilities of current applications. Today's rendition of the System Center Capacity Planner provides support for modeling Windows Server as well as Microsoft Exchange messaging environments, Microsoft Office SharePoint Server (MOSS) environments, Windows SharePoint Services (WSS) environments, and System Center Operations Manager 2007 (SCOM) environments.

Microsoft continues to add more modeling components to the System Center Capacity Planner to keep up with the addition of new products and new server models available.

What to Expect in the System Center Capacity Planner Chapter

In this book, a single chapter is dedicated to the System Center Capacity Planner product. Chapter 17, "Using System Center Capacity Planner for Predeployment Planning," covers what SCCP is, how it fits into the modeling assessment for applications, and the step-by-step process of running models and simulations as well as how to read and understand the reports generated.

System Center Capacity Planner 2007 is a helpful tool to run either proactive planning or reactive assessment simulations to determine or to confirm the capacity of servers for given applications. Jump to Chapter 17 of this book for specific information and deployment and configuration guidance on how SCCP can be best leveraged in your enterprise.

Understanding System Center Mobile Device Manager

System Center Mobile Device Manager is a product that Microsoft has been selling for the past few years. The current rendition of the product is System Center Mobile Device Manager (MDM) 2008 SP1. MDM provides tools to manage Windows Mobile devices in the enterprise, such as mechanisms to patch and update mobile devices, to inventory and track mobile devices, to enforce policies on mobile devices in terms of password change-control policies, and the like. The Mobile Device Manager console, shown in Figure 1.16, is the main menu for the MDM 2008 product.

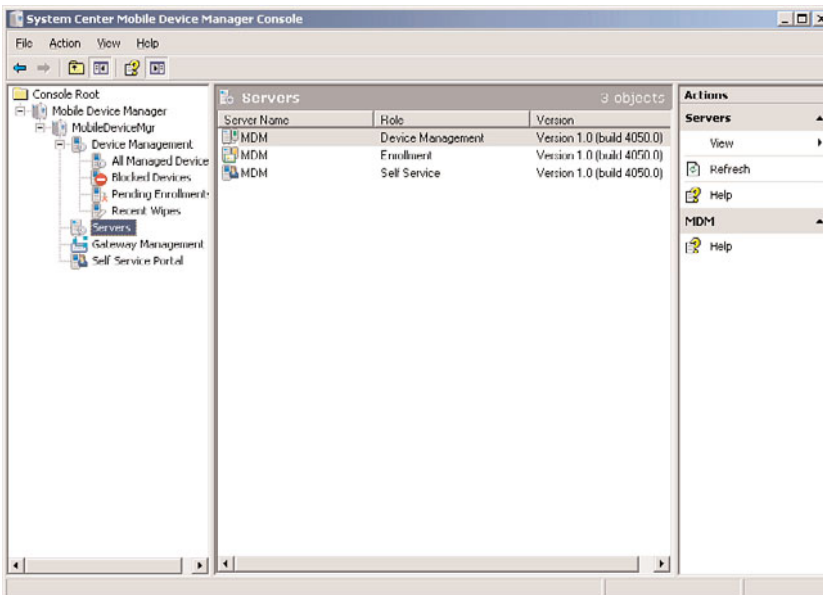


FIGURE 1.16 System Center Mobile Device Manager console.

Business Solutions Addressed by System Center Mobile Device Manager

Just a few years ago, a mobile device was usually just a mobile phone that a user would occasionally make phone calls on when they were out of the office. However, in the past couple of years, mobile phones have become the primary communications device for many users. Mobile phones are no longer just for making and receiving phone calls, but also act as email clients, web browsers, or even information access systems to acquire, store, and manage files and documents over the Internet.

Additionally, as these mobile devices do more, what used to be \$50 mobile phones that were not important to inventory and track in a network are now \$299 or \$399 devices that many times cost as much as a full-blown laptop or desktop these days. As such, organizations are inventorying the devices and tracking them as assets in the enterprise.

System Center Mobile Device Manager helps organizations keep track of their mobile assets as well as helps users maintain the privacy and security of the information stored on the mobile devices. With users synchronizing email messages to the mobile devices, or remotely accessing documents or spreadsheets and viewing the data on the mobile device, MDM needs to help organizations protect and secure potentially confidential or legally protected information.

Major Features of System Center Mobile Device Manager

The System Center Mobile Device Manager 2008 SP1 product provides a whole series of features and functions specific to the management of mobile devices; some of the major features in the product are as follows:

- ▶ **Device provisioning**—MDM helps administrators provision or set up a mobile device for users. Beyond just creating a user profile for the mobile device user to access and synchronize their emails and contacts, MDM's process of provisioning helps IT personnel lock down the device, uninstall unnecessary applications, encrypt content on the mobile device, enforce security on the mobile device, and provide secured (VPN) access from the mobile device into an organization's business resources.
- ▶ **Device inventory and tracking**—MDM also keeps track of mobile devices by keeping track of device serial numbers, validating that the device still exists and is active in the environment, and transferring serial numbers and asset tag information between users when a device changes from one individual to another in an organization.
- ▶ **Active updates and device management**—MDM also has the ability to push updates to a mobile device. Although many organizations pay little attention to the patching and updating of mobile devices in the enterprise, with the proliferation of mobile devices and the complexity of the software and applets available for mobile users to install and use on their mobile devices, performing periodic patching and updating of devices is critical. MDM provides the mechanism to update systems "over the air."
- ▶ **Password and PIN control**—The password and PIN control configuration options allows for changing security settings of mobile devices all from the centralized MDM console.
- ▶ **Self-service management**—The self-service management function of MDM, shown in Figure 1.17, allows a user to self-enroll new devices and submit requests for management options for their mobile device in a self-service web portal screen.
- ▶ **Device wipe and deprovisioning**—If a user loses their mobile device, MDM can send a "poison pill" to the device and wipe the data off the device and completely reset the device's configuration. This is important as a user who loses their device with sensitive emails or confidential file data is subject to the same laws and regulations that protect privacy of protected data, and as such, organizations need a process where device security can address laws and regulations around data protection.

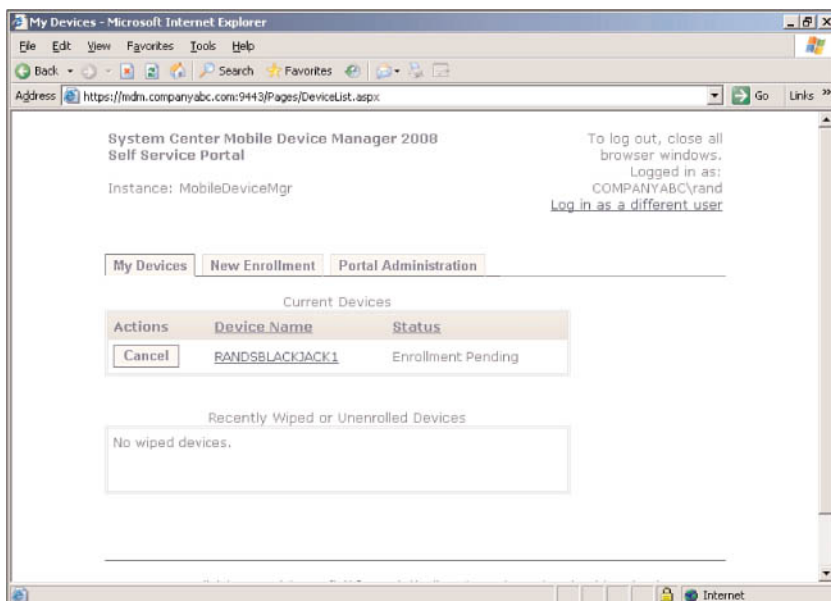


FIGURE 1.17 Self-service enrollment capabilities of MDM.

Background on System Center Mobile Device Manager

System Center Mobile Device Manager has been available for the past couple of years initially as a tool to simply provision and deprovision mobile devices. With the release of System Center Mobile Device Manager 2008 SP1, more functionality was added to better help administrators manage and support mobile devices in the enterprise. Mobile Device Manager today supports managing Windows Mobile v6.1 or higher devices utilizing Active Directory 2003 or Active Directory 2008 with specific policy push and security management control capabilities that organizations can leverage in their process to keep mobile devices managed and protected similar to servers and other client systems in the environment.

What to Expect in the System Center Mobile Device Manager Chapter

In this book, a single chapter is dedicated to the System Center Mobile Device Manager product. Chapter 18, "Using Mobile Device Manager to Manage Mobile Devices," covers what's in MDM, how administrators can install MDM, best practices at creating MDM policies, and how users can take advantage of MDM to self-service manage and support their mobile devices.

System Center Mobile Device Manager 2008 SP1 is a very helpful product for organizations looking to manage their Windows Mobile devices. Jump to Chapter 18 of this book for specific information and deployment and configuration guidance on how MDM can be best leveraged in your enterprise.

Understanding System Center Essentials

System Center Essentials is a standalone product focused on mid-sized organizations with fewer than 500 users and 50 servers. Rather than setting up a full-blown version of System Center Configuration Manager to patch and update systems, a full-blown version of System Center Operations Manager to monitor systems, and a full-blown version of Virtual Machine Manager to manage virtual guest sessions, System Center Essentials includes all of the major features in a single package.

The System Center Essentials 2010 console, shown in Figure 1.18, provides the main menu for all of the features and functions in Essentials 2010.

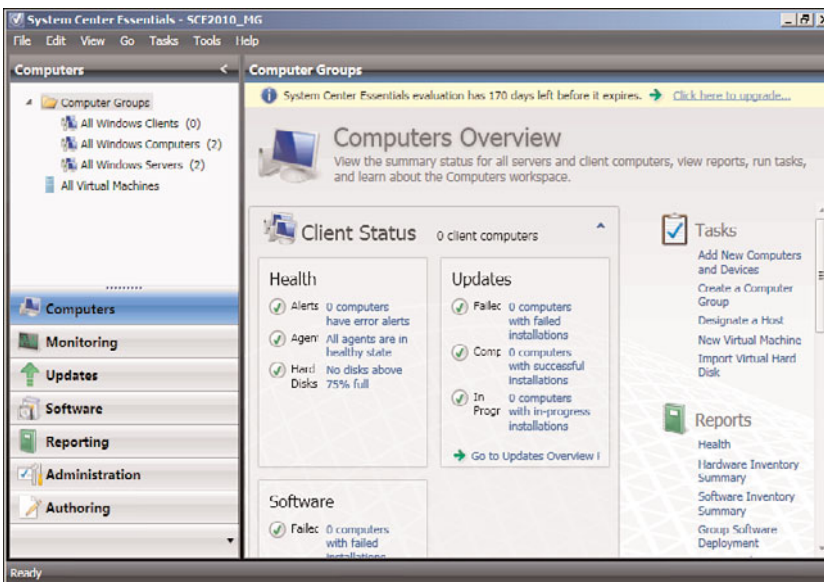


FIGURE 1.18 System Center Essentials console.

Business Solutions Addressed by System Center Essentials

For mid-sized organizations with limited personnel, the thought of setting up three or four management tools and then managing the management tools places the organization in the challenging situation of having management tools take more to manage than supporting the actual servers and systems themselves. Effectively, System Center Essentials helps organizations focus on managing the applications and not on managing the management tool.

System Center Essentials 2010 allows the administrator to complete business-critical tasks. One such task is tracking servers and system assets, as well as administering and managing

systems. To shorten the time from deployment to simplified management, System Center Essentials has built-in wizards that help an administrator set up and perform key tasks faster and easier. With a limited set of features, IT personnel can focus on key management factors, not become loaded down with a lot of large, enterprise-focused features not used by smaller businesses.

Major Features of System Center Essentials

System Center Essentials 2010 is an incredible tool that required Microsoft to make hard choices on what features to include that are valuable to administrators of small and mid-sized enterprises, but not overwhelm the administrators with too many features and functions that take away from the simplistic goals of the product. Some of the major features in the product are as follows:

- ▶ **Asset tracking**—All organizations, large or small, need to know what assets the organization has as well as keep track of the assets. System Center Essentials inventories systems in the environment and tracks the inventory so that when systems are added or inventory is removed, the administrator is notified.
- ▶ **Patching and updating**—Any organization hit with a virus or worm knows that patching and updating systems on a regular basis is critical. System Center Essentials provides an automatic mechanism to identify systems and keeps those systems patched and updated.
- ▶ **Software distribution**—The ability to push out new software or even push out service packs or updates is a core component of SCE. Although patches and updates are typically small file updates, software distribution involves scheduling and managing larger updates, such as 80MB service pack updates or 300MB product upgrades. SCE has the ability to package up applications and automatically push them to managed systems in the environment.
- ▶ **Remote support**—When a user has a problem with their system, the last thing an IT staff member needs to do is get up, track the user down, and provide face-to-face support when all the user does is sit and look over the IT personnel's shoulder. Instead, SCE provides remote-support capabilities so that the IT help desk or support individual merely launches a remote-control agent and takes control of the user's system to provide remote support and assistance.
- ▶ **Proactive monitoring and alerting**—Essentials 2010 monitors servers and generates alerts and proactively resolves system problems based on actual user experience. The monitoring notifies the IT administrator when problems occur. The monitoring screen is shown in Figure 1.19.
- ▶ **Virtual host management**—As organizations of all sizes are virtualizing their servers, SCE has the virtual host management capabilities of Virtual Machine Manager built in. This feature in SCE allows an administrator to manage and support virtual guest sessions right from the SCE console.

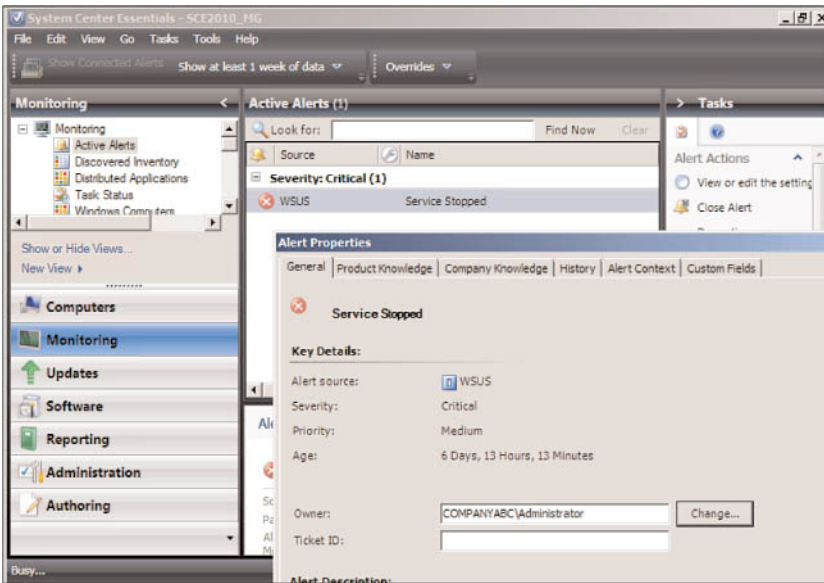


FIGURE 1.19 Server monitoring in System Center Essentials.

- **Physical-to-virtual (P2V) conversions**—One of the most commonly used features in the full-blown System Center Virtual Machine Manager product is the P2V function. P2V converts a physical server in an environment to a virtual guest session.
- **Reporting**—Lastly, SCE has critical reporting capabilities built in so that reports can be generated and printed on network assets, the patch and update status of systems, service-level agreement uptime reports, access and password violation tracking reports, and the like. These reports are necessary for an organization to understand the status of systems and security in the environment, and when required by auditors or regulators, to have the information immediately available to share with the proper authorities.

Background on System Center Essentials

System Center Essentials is a relative newcomer to the System Center family of products with the initial release coming out only in 2007. The product has not drastically changed since the 2007 release, other than the update and addition of more components into the product to have the current version of the product. System Center Essentials 2010 supports the capabilities of the 2007 edition plus the addition of virtualization management.

The whole premise of the product was to make a simplified set of tools an administrator could leverage to help them manage servers and client systems in the enterprise. The core components that provide system inventory, patching, updating, monitoring, and alerting are the core components in Essentials 2007 and are carried over to Essentials 2010.

The biggest improvements in the product have been the addition of new wizards and automated process controls that continue to simplify the use and administration of the product.

What to Expect in the System Center Essentials Chapter

In this book, a single chapter is dedicated to the System Center Essentials 2010 product. Chapter 19, “Using System Center Essentials for Midsized Organizations,” covers everything from how to install and configure SCE to the use of SCE 2010 for patching, updating, distributing software, monitoring, alerting, and managing virtual systems.

System Center Essentials 2010 is an excellent tool for organizations with fewer than 500 users and 50 servers to get all of the key benefits found in the other Microsoft System Center products, but from a single server installation and console. Jump to Chapter 19 of this book for specific information and deployment and configuration guidance on how SCE can be best leveraged in your enterprise.

Understanding System Center Licensing

System Center is sold and licensed as individual products or as a suite with several System Center components bundled together. It is always best to visit the Microsoft website (<http://www.microsoft.com/systemcenter/en/us/pricing-licensing.aspx>) to best understand the current licensing scheme as the licensing model changes, or better yet, contact a licensing specialist who can provide information on special discounts that apply based on your organization’s purchasing and licensing contract.

However, in general, the core System Center products, including System Center Configuration Manager, System Center Operations Manager, System Center Data Protection Manager, System Center Virtual Machine Manager, and System Center Service Manager, are all sold as a server license along with a client access or operating system environment license.

The server license is typically the main license for the application itself. As an example, SCCM and SCOM require a server to host the software, and, thus, the server itself needs to have an SCCM or SCOM server license. Likewise, SCCM and SCOM also have client systems associated with the servers that are managed; in the case of SCCM, which patches, updates, and manages workstations, an SCCM client license is required for each client system under management. For SCOM, because frequently it is a server that is being monitored and managed, the SCOM client license is actually a management license for the target server being managed.

In the case of System Center Virtual Machine Manager, there are no specific “clients” associated with the product, only virtual host servers and virtual guest sessions. Microsoft uses what they call an operating system environment (OSE) license as the target destination license for VMM.

Core Client Access Licenses

For products that have client access licenses like SCCM, Microsoft bundles licenses within their client license platform. As an example, organizations that have a core client access license, or CoreCAL, that provides them rights to use Windows, standard Exchange features, and standard SharePoint features, the CoreCAL also includes a license for SCCM. Pretty much every mid- and large-size enterprise has an enterprise agreement with the CoreCAL and, as such, these organizations already own the client license for SCCM. All the organization needs to do is purchase a server license for SCCM to be able to set up a full SCCM-managed environment.

Server Management Suite Volume Licensing

For products where Microsoft licenses the products based on servers, an organization can purchase a Server Management Suite license. More details on Server Management Suite license are available at <http://www.microsoft.com/systemcenter/en/us/management-suites.aspx>.

But, in general, there is the System Center Server Management Suite Enterprise (SMSE) and the System Center Server Management Suite Datacenter (SMSD) licenses. The SMSE provides a license in an environment where virtualization is used where the SMSE license covers the licensing of System Center Configuration Manager, System Center Operations Manager, System Center Data Protection Manager, and System Center Virtual Machine Manager for the physical host server as well as up to four virtual guest sessions on the system running System Center products.

The SMSD license covers all of the same System Center products, but for a flat fee per processor, it covers ALL of the guest sessions running on a single physical host server.

Microsoft has several discount levels on licensing and it is best to discuss the licensing requirements as well as specific license pricing with an organization that can assess the licensing pricing level of your organization.

Summary

This first chapter of the book was intended to provide you, the reader, with a background of the various System Center products available, how the products fit into the management scheme of an organization, and what to expect in the subsequent chapters in this book.

Overall, the life cycle in an enterprise has a system operating system deployed on a system using System Center Configuration Manager that also patches and updates the system and keeps the system in a standardized configuration. The System Center Operations Manager product then monitors the system, whether a server or a client system, and proactively alerts administrators of any pending problems.

The System Center Data Protection Manager backs up server and application data and provides the ability for the administrator or even an end user to recover information based on as little as 15-minute increments of time. In addition, the System Center Virtual Machine Manager product helps to manage physical and virtual server systems, including the conversion of physical systems to virtual guest sessions as well as intelligently placing guest sessions on physical servers with the most available capacity.

The overall tool that helps an organization manage their environment is the System Center Service Manager that provides incident management, change control, and consolidated reporting for servers and client systems within the environment.

Enterprises that do proactive planning and modeling can leverage the System Center Capacity Planner tool, and those organizations with mobile devices can inventory, control, provision, and deprovision mobile devices with the System Center Mobile Device Manager product.

Finally, for smaller organizations that want the key capabilities available in the System Center family of products but really only need the most common features used in organizations, they can get the System Center Essentials product. System Center Essentials provides patching, updating, monitoring, alerting, and virtual system management for organizations with fewer than 500 users and fewer than 50 servers.

All of these tools are available to be purchased individually or are bundled in suites and can be purchased together. The focus of this book is to help you, the reader, better understand not only what the products are, but how the products tie together so that you can develop an overall strategy for managing and administering your servers and client systems throughout your enterprise.

Best Practices

The following are best practices from this chapter:

- ▶ Utilize the capabilities built in to System Center Configuration Manager to deploy the base operating system for both servers and client systems in your enterprise.
- ▶ Use templates and standard configurations so that all system images and all applications deployed use the same settings and parameters for organizational consistency.
- ▶ Leverage the System Center Configuration Manager product's Desired Configuration Management (DCM) if you want to enforce policy-based system standards.
- ▶ Implement the Internet Client in System Center Configuration Manager for remote and mobile systems that need to be managed, but rarely or never VPN or directly connect to the network backbone.
- ▶ Use System Center Operations Manager to proactively monitor systems and alert IT of any pending problems.
- ▶ Utilize the event correlation capabilities of SCOM to more easily isolate system problems and errors to root causes of the problems.

- ▶ Implement the application-monitoring capabilities of SCOM to monitor specific application sessions critical to the safe operations of an application server.
- ▶ Back up servers and applications using System Center Data Protection Manager using incremental timed backups for more flexibility on recovery of information.
- ▶ Choose to back up secondary systems in an environment (such as the second node of a cluster) so as to not impact the performance of the primary server during a backup.
- ▶ Consider pushing DPM backup data to a cloud service provider and eliminate tapes altogether in an enterprise by having short-term backups reside on the DPM server and long-term backups reside in the cloud.
- ▶ Use the System Center Virtual Machine Manager product to manage physical host servers of both Microsoft Hyper-V and VMware host systems for centralized virtual host management.
- ▶ Use the physical-to-virtual (P2V) tool in VMM to convert physical servers into virtual guest sessions.
- ▶ Use the virtual-to-virtual (V2V) tool in VMM to convert virtual guest sessions (either Hyper-V or VMware) into Hyper-V virtual guest sessions.
- ▶ For organizations that delegate administration to multiple levels of administrators, use the administration delegation feature in VMM to distribution rights to multiple administrators.
- ▶ To allocate virtual host resources to users to create guest sessions as they require, use the Self-Service Portal feature in VMM to assign usable templates and configuration options for users.
- ▶ Implement the System Center Service Manager product to centralize incident management in the organization and provide help desk controls for IT personnel throughout the organization.
- ▶ Leverage the change-control capabilities in SCSM to ensure and to enforce the organization's change-control policies in the enterprise.
- ▶ Provide self-service capabilities to users so they can submit problems and incidents themselves and can check to see if there are known fixes to the problems where they can fix the problem quickly and easily themselves.
- ▶ Use the System Center Capacity Planner tool to model system configurations for file systems, SharePoint, Exchange, and SCOM environments to properly size and scope servers and server roles for these applications.
- ▶ Use the System Center Mobile Device Manager product to more easily manage mobile devices, including provisioning and deprovisioning devices.
- ▶ When a mobile device is lost, use the device wipe capability found in MDM to wipe any and all data on the device and prevent the information from getting in the wrong hands.

- ▶ To provide secure access from mobile devices to the network, use the Mobile VPN capability in MDM to allow a secured and protected connection to the network.
- ▶ For organizations with fewer than 500 users and 50 servers, consider deploying and using System Center Essentials for patching and updating systems, deploying software, monitoring, and managing virtual systems to simplify the installation, administration, and management of systems.

Index

A

Access Violation reports, 523

Account Management reports, 523

accounts

Action Agent, 282

Client Push Installation, 84

Data Warehouse Reader, 282

Data Warehouse Write Action, 282

Domain Join, 84

Local Administrator, 282

Management Server Action, 282

Network Access, 84

Non-Privileged User, 464

OS Capture Account, 84

Privileged User, 462-463

RunAs, 283

SDK and Configuration service
accounts, 282

UNIX Action Account profile, assigning Linux
Non-Privileged Users to, 464

UNIX Privileged Account profile, assigning
Linux Privileged Users to, 464-465

ACS (Audit Collection Services)

ACS Reporting, 276-277

audit collection database, 275-276, 287

audit collector, 275

audit forwarder, 274

OpsMgr 2007 R2 ACS (Audit Collection
Services) install, 337-343

reports

Access Violation reports, 523

Account Management reports, 523

custom reports, 525-528

explained, 522-523

Forensic reports, 523

generating, 524-525

Planning reports, 523-524

Policy reports, 524

System Integrity reports, 524

Usage reports, 524

Action Agent account, 282

Active Alerts view, 447, 457

Active Directory. See AD (Active Directory)

Active Directory Management Pack

client monitoring, 426-427

configuring, 423-424

domain controller performance collection,
431-433

explained, 423

replication monitoring, 427-431

reports, 437-438

tasks, 436-437

views, 432-436

activities

activity prefixes, 813

explained, 810-811

MAs (manual activities), 831-832

RAs (review activities), 828

returning to, 825-828

Activity Distribution report, 841

Activity Management Report Library, 841

AD (Active Directory)

Active Directory connector deployment,
747-748

Active Directory Management Pack

client monitoring, 426-427

configuring, 423-424

domain controller performance
collection, 431-433

explained, 423

replication monitoring, 427-431

reports, 437-438

tasks, 436-437

views, 432-436

configuring, 134-135

configuring Remote Assist with, 949-950

extending AD schema, 56-57, 133-134

in MDM (Mobile Device Manager), 871-872

site topology, 116-117

AD Generated Response Task, 436

**AD Users and Computers Snap-in Console
Task, 436**

ADConfig command, 878-879

Add Hosts Wizard, 657-659

Additional Properties page

Convert Physical Server Wizard, 677

Convert Virtual Server Wizard, 682

Deploy Virtual Machine Wizard, 696-697

AddNewClusteredVM.ps1 script, 617-618

AddNewStandAloneVM.ps1 script, 617-618

administration

DPM (Data Protection Manager) 2010

Administrator Console, 575-577

custom volumes, 579-580

data recovery, 580-581

Management Shell, 577-578

OpsMgr

daily tasks, 368-369

explained, 390

file exclusions for antivirus and defrag-
mentation applications, 376-377

importing management packs, 369-371

management pack updates, 371-372

Management Packs tree item, 393,
399-400

notification and alert tuning, 372-376

Notifications tree item, 393-395

Pending Management tree item,
392-393

performance monitoring, 395-399

Web console performance view time
frame, 377-378

System Center Essentials

monthly tasks, 983-984

regular tasks, 981

weekly tasks, 982-983

Administration option (SCE), 935-937

Administrator Console (DPM), 575-577

Administrator Console (VMM)

explained, 631, 666-667

hardware requirements, 642

installing, 654-656

software requirements, 642

supported operating systems, 642

Administrator role (VMM)

defined, 684

managing, 684-686

Administrator Tools (MDM), installing, 885-886**ADSI Edit**

- ADSI Edit Snap-in Console Task, 436
- creating System Management container with, 134-135

Advertised Programs Client Agent, 96, 174, 180
advertisements, 58, 185

Agent Health view, 458**Agent Proxy, configuring, 362-363****agents**

- Advertised Programs Client Agent, 96, 174, 180
- Agent Proxy configuration, 362-363
- agent restart recovery, 363-364
- Computer Client Agent, 96, 174, 178-181
 - controlling bandwidth, 180-181
 - network access and policy retrieval, 178
 - user experience, 179
- Configuration Manager Agent package, 206-207
- configuring to use certificates, 358
- Desired Configuration Management Client Agent, 96
- explained, 263-265
- Hardware Inventory Client Agent, 96
- installing, 166-167
 - on DMZ servers, 356-357
 - on domain-attached systems, 973-974
 - Firewall Rule exceptions, 978-979
 - on non-domain joined systems, 974-977
- manual agents, 359-360
- Mobile Device Client Agent, 96
- Network Access Protection Client Agent, 73
- Remote Tools Client Agent, 97
- security, 280
- Software Inventory Client Agent, 97
- Software Metering Client Agent, 97
- Software Update Client Agent, 97
- Software Updates Client Agent, 196-197
- UNIX/Linux agents, 349-352
- VMM Agent
 - explained, 632
 - installing, 657-661

- website monitoring agents
 - creating, 961-963
 - response time alerts, 963-964
- Windows agents, 343-345

AI (Asset Intelligence)

- AI catalog, 235-236, 245-246
- Asset Intelligence Synchronization Points
 - enabling, 236
 - explained, 71-72, 158
- CAL license tracking, 241-242
- explained, 61-63, 234-235
- logon auditing, 242-243
- report categories, 247
- reporting classes, 236-241
- System Center Online Services, 246-247

AIUpdateSvc.log log file, 236**alert forwarders, configuring, 346-349****Alert Logging Latency report, 513, 515-516****Alert reports, 506-508**

Alert view (Operations Manager console), 389
alerts, 44

- alert forwarders, 346-349
- Alert Logging Latency report, 513, 515-516
- Alert reports, 506-508
- alert tuning, 405-408
- creating incidents with, 777-780
- Daily Alert report, 513, 519-521
- explained, 258
- generating, 261
- Most Common Alerts report, 514-515
- priority levels, 365
- response time alerts, 963-964
- severity levels, 365
- in System Center Essentials, 942
- tuning, 372-376

All Open Unassigned Incidents folder, 784**All Performance Data view, 458**

Allow BITS Download Outside of Throttling
Window setting (Computer Client Agent), 180

Allow Bluetooth setting (Exchange Server
2007), 905

Allow Browser setting (Exchange Server
2007), 905

Allow Camera setting (Exchange Server 2007), 905

Allow Consumer Mail setting (Exchange Server 2007), 905

Allow Desktop Sync setting (Exchange Server 2007), 905

Allow HTML E-mail setting (Exchange Server 2007), 905

Allow Internet Sharing setting (Exchange Server 2007), 905

Allow non-provisionable devices setting (Exchange Server 2007), 906

Allow POPIMAP Email setting (Exchange Server 2007), 906

Allow Remote Desktop setting (Exchange Server 2007), 906

Allow Simple Password setting (Exchange Server 2007), 906

Allow S/MIME Software Certificates setting (Exchange Server 2007), 906

Allow Storage Card setting (Exchange Server 2007), 906

Allow Text Messaging setting (Exchange Server 2007), 906

Allow Unsigned Applications setting (Exchange Server 2007), 906

Allow Wi-Fi setting (Exchange Server 2007), 906

Allow IIRDA setting (Exchange Server 2007), 905

Alphanumeric Password Required setting (Exchange Server 2007), 906

analyzing

incidents, 784-787

problems, 797-798

announcements, publishing, 787-788

antivirus applications, file exclusions for, 376-377

application monitoring, 17-18

Application page (Model Wizard), 858-859

applications, disabling, 901-902

Approved Application List setting (Exchange Server 2007), 906

approving

packages, 897-898, 959

RAs (review activities), 828

updates, 954-956

Asset Intelligence (AI). See AI (Asset Intelligence)

assets

AI (Asset Intelligence). See AI (Asset Intelligence)

asset management

explained, 61

hardware/software inventory, 61-62

managing, 158

tracking, 10, 44

assigning incidents, 783-784

Attachments Enabled setting (Exchange Server 2007), 906

audit collection database, 275-276

Audit Collection Services. See ACS (Audit Collection Services)

audit collector, 275

audit forwarder, 274

audits

ACS (Audit Collection Services). See ACS (Audit Collection Services)

audit collector, 275

audit forwarder, 274

logon auditing, 242-243

Authoring Console, 481

Authoring option (SCE), 937

autodiscover (SCE), 938-939

automatic client installation, 167

automatic placement of VMs (virtual machines), 692-693

automatically deploying software, 193-194

Availability reports, 261-262, 497-498, 508-512

B

Back Up Database dialog box, 754

backing up

ConfigMgr, 85-86

with DPM (Data Protection Manager) 2010.

See DPM (Data Protection Manager) 2010

OpsMgr

backup schedules, 378

explained, 287-289

- IIS 6.0 metabase backup, 383-384
- IIS 7.x configuration backup, 385
- OperationsManager database, 379-380
- OperationsManagerAC database backup, 383-384
- OperationsManagerDW database backup, 381-383
- RMS encryption key backup, 380-381
- Service Manager
 - backup schedules, 753-754
 - encryption key, 756
 - ServiceManager database, 754-756
- System State, 587
- tape-based backup technologies, 545-546

bandwidth

- controlling with Computer Client Agent, 180-181
- controlling with site deployment, 93-94
- OpsMgr requirements, 291-293

baselines

- applying to collections, 251-252
- defining, 251
- monitoring, 246-253

BITS tab (Computer Client Agent), 179

BITS-enabled Distribution Points, 73

blocking device connections, 892-893

boot images, configuring, 209

boundaries

- configuring, 153-155
- establishing, 94-96

Branch Distribution Points, 73

BranchCache, 74

C

CAL license tracking, 241-242

calculating storage requirements, 557-558

capacity models, 38-39

- basic infrastructure requirements, 851
- capabilities, 850
- constructing, 846

- creating with Model Wizard, 853-860

- Application page, 858-859

- Client-Only Sites page, 854-855

- Hardware page, 857-858

- Mailbox Sites page, 853-854

- Model Summary page, 859-860

- Networks page, 855-856

- editing with Model Editor, 860-862

- simulations, 862-863

capturing performance information into OpsMgr, 396-397

CAS role monitor and rule sync times, 441

CAS Synthetic Transaction State view, 447

catalogs (AI), 235-236, 245-246

ccm.log file, 166

CCR (Client Configuration Request) files, 167

CDP (Continuous Data Protection), 547-548

CDP (CRL Distribution Point) settings, 119-120

Central Sites

- Configuration Manager 2007 R2 upgrade, 147

- configuring WSUS website for SSL, 139-140
- explained, 68, 114, 137-138

- installing, 143-145

- requesting Document Signing certificate, 140-143

- requesting OS Deployment certificate, 143

- reviewing site status, 146

- validating installation, 145-147

- WSUS 3.0 SP2, 138-139

Certificate Auto-Enrollment GPO, 120-122

Certificate Services website for SSL, 128-129

certificates, 120

- Certificate Auto-Enrollment GPO, 120-122

- Certificate Services website for SSL, 128-129

- Client Authentication certificate template, 122-123

- Client Certificate, 103, 115

- ConfigMgr Native mode requirements, 102

- Document Signing Certificate

- explained, 103, 115, 126

- requesting, 140-143

- monitoring DMZ servers with
 - configuring agents to use certificates, 358
 - creating certificate templates, 353
 - explained, 352-353
 - installing agents on DMZ servers, 356-357
 - requesting certificates from root CA for mutual authentication, 355-356
 - requesting root CA certificates, 353-355
- OS Deployment certificate
 - explained, 124
 - requesting, 143
- publishing certificate templates, 126-127
- root CA certificates, installing on SCE server, 974-975
- securing DMZ servers with, 283
- Server Authentication certificate templates, 124-126
- Server Certificate, 103, 115
- templates
 - creating, 353
 - explained, 103-104
- certreq command, 882**
- Certreq TechNet site, 104**
- Certreq.exe command-line tool, 104, 119**
- CFS (Sanbolic Clustered File System), 639-640**
- change management**
 - activities, 810-811
 - activity prefixes, 813
 - MAs (manual activities), 831-832
 - RAs (review activities), 828
 - change requests
 - adding reviewers to change requests, 824-825
 - automatic notifications of change request status, 833-834
 - closing, 832-833
 - creating from configuration items, 818
 - creating from incidents/problems, 819
 - creating from scratch, 817
 - creating from Self-Service Web Portal, 819-821
 - explained, 810
 - holding, 825-826
 - investigating change requests, 822-824
 - resuming, 826-827
 - returning to activities, 690-828
 - templates, 814-815
 - workflows, 815-816
- change settings
 - activity prefixes, 813
 - Change Request Prefix, 811-812
 - file attachment limits, 812-813
- CIs (configuration items)
 - creating change requests from, 818
 - deleting, 836-838
 - explained, 835
 - searching, 836-837
- explained, 34, 807-810
- reports
 - Activity Management Report Library, 841
 - Change Management Report Library, 840-841
 - Configuration Management Report Library, 842-843
 - explained, 838-839
 - Service Manager report controls, 839
- workflows, 815-816
- Change Management KPI Trend report, 840**
- Change Management Report Library, 840-841**
- Change Request Prefix, 811-812**
- change requests**
 - adding reviewers to, 824-825
 - automatic notifications of change request status, 833-834
 - closing, 832-833
 - creating
 - from configuration items, 818
 - from incidents/problems, 819
 - from scratch, 817
 - from Self-Service Web Portal, 819-821
 - explained, 810
 - holding, 825-826
 - investigating, 822-824
 - resuming, 826-827
 - returning to activities, 825-828
 - templates, 814-815
 - workflows, 815-816
- channels, 366**

Check Catalog (DBCC) task, 459

Check Database (DBCC) task, 459

Check Disk (DBCC) task, 459

child Primary Sites deployment, 148

Cls (configuration items)

deleting, 836-838

explained, 835

searching, 836-837

classes

AI (Asset Intelligence) reporting classes,
236-241

Win32Reg_CompanyABC_Warranty,
validating, 227

Client Access Server Active Alerts view, 447

Client Access Server Monitoring, 445-447

Client Access Servers State view, 447

Client Agents

configuring for inventory collection

explained, 221-222

Hardware Inventory Client Agent,
222-223

Software Inventory Client Agent, 222

Desired Configuration Management Client
Agent, 247-248

enabling, 157

Software Metering Client Agent, 234

Client Alerts view, 434

**Client Authentication certificate template, creat-
ing, 122-123**

Client Certificate, 103, 115

Client Configuration Request (CCR) files, 167

Client Health Components, 70-71

Client Installation Methods, 164

Client Performance Overview view, 435

Client Push Installation accounts, 84

Client RPC Latency view, 450

Client RPC Succeeded view, 450

Client State view, 435

Client-Only Sites page (Model Wizard), 854-855

clients. See also specific clients

automatic client installation, 167

Client Health Components, 70-71

Client Installation Methods, 164

client roaming, 56-57

client schedules, 104-105

controlling client access to regional servers,
162-163

creating Registry keys on, 223-224

discovery methods, 91, 164-165

explained, 66-67

locating content with, 174-176

monitoring, 17

port requirements, 82-83

site assignment, 107

closing change requests, 832-833

cloud-based storage, 547

clusters

explained, 285-286

host clusters, 667-668

protecting data on, 585

VMM support for, 634-635

**CMDB (configuration management database),
711**

cmdlets

Disable-NotificationSubscription, 394

Enable-NotificationSubscription, 394

Get-Help, 578

Get-NotificationSubscription, 394-395

New-DeviceDiscoveryConfiguration, 489

collecting inventory, 220, 960-961

collections

configuring, 165-166

creating, 182-185

designing, 90-91

maintenance windows, 184

command shells

OpsMgr, 272-273, 391-392

VMM (Virtual Machine Manager), 670-671

commands. See specific commands

communication ports (OpsMgr), 280-281

compliance, monitoring, 246-253

Component Servers, 114

Component Status page (ConfigMgr), 145-147

Computer Client Agent

controlling bandwidth, 180-181

explained, 96, 174, 178-181

network access and policy retrieval,
178-181

user experience, 179

Computer Details report, 842

computer discovery. See *discovery*

Computer Inventory report, 842

computer management (ConfigMgr), 177-178

Computer Management task, 413

**computers, adding/modifying with Capacity
Planner Hardware Editor, 852**

Computers Diagram view, 466

**Computers option (SCE management
console), 931**

Computers view, 457

ConfigMgr

AD (Active Directory)

configuring, 134-135

extending AD schema, 56-57, 133-134

site topology, 116-117

agents

Advertised Programs Client Agent, 180

Computer Client Agent, configuring,
178-181

installing, 166-167

Software Updates Client Agent, 196-197

AI (Asset Intelligence). See *AI (Asset
Intelligence)*

architecture, 115-116

asset management. See *assets*

asset tracking, 10

business solutions addressed by, 9-10

Central Site deployment

Configuration Manager 2007 R2
upgrade, 147

configuring WSUS website for SSL,
139-140

explained, 68, 138

installing Central Site Server, 143-145

requesting Document Signing certificate,
140-143

requesting OS Deployment certificate,
143

reviewing site status, 146

validating installation, 145-147

WSUS 3.0 SP2 installation, 138-139

certificate deployment

Certificate Auto-Enrollment GPO,
120-122

Certificate Services website for SSL,
128-129

Client Authentication certificate
template, 122-123

Document Signing Certificate
template, 126

explained, 120

OS Deployment certificate, 124

publishing certificate templates,
126-127

Server Authentication certificate
templates, 124-126

child Primary Site deployment, 148

Client Health Components, 70-71

clients

automatic client installation, 167

client installation methods, 164

client roaming, 56-57

client schedules, 104-105

discovery methods, 164-165

explained, 66-67

locating content with, 174-176

collections

configuring, 165-166

creating, 182-185

maintenance windows, 184

components summary, 65-66

computer management, 177-178

Configuration Manager connector
deployment, 752-753

configuring hierarchy

boundaries, 153-155

Client Agents, 157

Distribution Points, 155

explained, 54-55, 148-149

FSP (Fallback Status Point), 151

IBCM (Internet-Based Client
Management), 156-157

RP (Reporting Point), 151-152

RSP (Reporting Service Point), 152-153

Site System roles, 149-150

SLP (Server Locator Point), 150-151

- console, 9
- content distribution
 - operating system deployment, 59-60
 - software distribution, 58
 - software update distribution, 59
- databases
 - explained, 219-220
 - sizing, 89-90
- DCM (Desired Configuration Management)
 - applying baselines to collections, 251-252
 - Client Agent, 247-248
 - defining configuration baselines, 251
 - defining configuration items to monitor, 248-251
 - explained, 63, 247-248
 - monitoring baselines and compliance, 246-253
- design considerations
 - bandwidth control, 93-94
 - boundaries, 94-96
 - client discovery and deployment, 91
 - client settings, 96-97
 - collections, 90-91
 - data flow, 97-98
 - disk performance, 98
 - multiple sites, 92
 - PXE Service Points (PSPs), 94
 - SAN versus DAS, 98-100
 - site-specific configuration settings, 92-93
 - SQL versions, 100-101
 - State Migration Points (SMPs), 94
 - user/group discovery, 91-92
- design scenarios, 107
 - large enterprise, 108-109
 - small and medium enterprise, 108
- Desired Configuration Management, 11
- disaster recovery, 85-86
- Distribution Points
 - BITS-enabled Distribution Points, 73
 - Branch Distribution Points, 73
 - BranchCache, 74
 - explained, 72-73, 181-182
 - Protected Distribution Points, 74
 - selecting, 190-191
 - Standard (SMB) Distribution Points, 73
- explained, 7, 50-53,
 - fault tolerance, 84-85
- FSP (Fallback Status Point), 74
- hardware requirements, 86-87
- Health Validator Point, 74-75
- history and revisions, 12-14
- IBCM (Internet-Based Client Management)
 - client site assignment, 107
 - explained, 105
 - requirements and limitations, 105-106
 - site system placement, 106-107
- IIS (Internet Information Services), 135-136
- Internet Client, 11
- inventory
 - configuring Client Agents for, 221-223
 - customizing hardware inventory, 223-226
 - IDMIF files, 221
 - inventory collection process, 220
 - NOIDMIF files, 221
 - validating inventory data, 227
 - viewing inventory data, 228
- Management Point (MP), 75
- and MDM (Mobile Device Manager), 78-79, 908-909
- Native mode
 - certificate requirements, 102
 - certificate templates, 103-104
 - explained, 79-80, 102
 - PKI (Public Key Infrastructure), 103
- network bandwidth requirements, 88-89
- operating system deployment
 - common scenarios, 204-205
 - creating software packages, 206-207
 - custom operating system images, 213-214
 - deployment technologies, 203-204
 - explained, 10, 160, 203
 - monitoring, 213
 - OS install packages, 207-210

- requirements, 205
- software distribution packages, 206
- troubleshooting, 212-213
- unknown computer support, 210-212
- Out-of-Band Service Point, 75
- patch management, 158-160
- patching/updating systems, 10-11
- PKI (Public Key Infrastructure), creating
 - deploying Enterprise Root CA, 118-120
 - explained, 118
 - validating Enterprise Root CA, 120
- Primary Site Server, 68
- Proxy Management Points, 55-56
- PSP (PXE Service Point), 75-76
- regional server infrastructure
 - controlling client access to regional servers, 162-163
 - deploying regional site components, 161-162
 - explained, 161
 - WDS (Windows Deployment Service), 161
- remote control, 10
- reporting
 - custom reports, 231
 - explained, 12, 64, 228-231
 - legacy reports, 231
 - Reporting Services reports, 231-234
 - software metering reports, 234-235
- roles, 113-115, 173-174
- RP (Reporting Point), 77
- RSP (Reporting Service Point), 77
- Secondary Sites, 55-56
- security
 - management console, 80-82
 - Mixed versus Native mode, 79-80
 - port requirements, 82-83
 - server communication, 80
 - service account security, 83-84
- Site Server databases, 69-70
- SLP (Server Locator Point), 77-78
- SMP (State Migration Point), 76
- SMS Provider, 68-69

- software distribution
 - configuring package programs, 189-190
 - configuring software sources, 186
 - creating software packages, 189
 - customizing installation, 187-188
 - deploying software automatically, 193-194
 - explained, 11, 185-186
 - monitoring software deployment, 195
 - publishing software, 191-192
 - selecting Distribution Points, 190-191
- software licensing data, importing, 243-245
- software metering
 - explained, 63, 234
 - reports, 234-235
 - Software Metering Client Agent, 234
- software requirements, 87-88
- SQL Server
 - installing, 130-132
 - local firewall configuration, 132-133
 - SQL service accounts, creating, 129
- SSL configuration, 136-137
- SUP (Software Update Point), 78
- System Center Online Services, 246-247
- update distribution
 - deploying software updates, 200-201
 - deployment templates, 197-198
 - explained, 196
 - managing update deployment, 201-202
 - monitoring software update deployment, 202-203
 - Software Updates Client Agent, 196-197
 - update lists, 198-199
- WebDAV configuration, 137-138
- WOL (Wake On LAN), 71
- configuration baselines**
 - applying to collections, 251-252
 - defining, 251
 - monitoring, 246-253
- configuration items. See CIs (configuration items)**
- Configuration Items (CIs) with Most Incidents report, 804**

Configuration Management Report Library, 842-843

Configuration Manager. See ConfigMgr
Configuration Manager Agent package, 206-207

configuration.mof file, editing, 225-226, 241-242

ConfigureSharePoint.exe utility, 606

configuring

AD (Active Directory), 134-135

agents to use certificates, 358

AI (Asset Intelligence)

AI catalog, 235-236

Asset Intelligence Synchronization Point, 236

logon auditing, 242-243

reporting classes, 236

alert forwarders, 346-349

boot images, 209

Certificate Services website for SSL, 128-129

change settings

activity prefixes, 813

Change Request Prefix, 811-812

file attachment limits, 812-813

channels, 366

Client Access Server Monitoring, 445-447

Client Agents for inventory collection

explained, 221-222

Hardware Inventory Client Agent, 222-223

Software Inventory Client Agent, 222

Client Installation Methods, 164

client monitoring, 426-427

cluster configuration, 285-286

collections, 165-166

Computer Client Agent, 178-181

network access and policy retrieval, 178-181

policy retrieval, 178-181

user experience, 179

ConfigMgr console

Client Agents, 157

Distribution Points, 155

explained, 149

FSP (Fallback Status Point), 151

IBCM (Internet-Based Client Management), 156-157

RP (Reporting Point), 151-152

RSP (Reporting Service Point), 152-153

Site System roles, 149-150

SLP (Server Locator Point), 150-151

DCM (Desired Configuration Management)

applying baselines to collections, 251-252

Client Agent, 247-248

defining configuration baselines, 251

defining configuration items to monitor, 248-251

explained, 247-248

monitoring baselines and compliance, 246-253

Desired Configuration Management, 11

discovery methods, 164-165

DPM (Data Protection Manager) 2010

disks, 563-564

protection agent deployment, 565-570

protection groups, 570-574

tape library, 564-565

IBCM (Internet-Based Client Management), 156-157

incident settings, 761

file attachment limits, 761-762

inbound email settings, 766-769

incident prefix, 761

Operations Manager Web console settings, 765-766

priority calculation, 762-764

resolution times, 764-765

Internet mail flow, 443-444

intraorganization synthetic transactions, 443-444

management packs

Active Directory Management Pack, 423-424

Cross Platform Management Packs, 461-465

Exchange 2007 Management Pack, 438-442

- Operations Manager Management Pack, 408-410
- SQL Server Management Pack, 455
- Non-Privileged User accounts, 464
- notifications
 - SMTP notification channel, 771-772
 - templates, 772-773
- OpsMgr
 - Agent Proxy configuration, 362-363
 - agent restart recovery, 363-364
 - Global Management Group Settings, 359-361
 - notifications and subscriptions, 364-367
- package programs, 189-190
- Privileged User accounts, 462-463
- problem settings
 - explained, 793
 - file attachment limits, 794
 - priority calculation, 795-796
 - problem prefix, 793
- Remote Assist, 947-948, 949-950
- Remote Desktop, 948-949
- response time alerts, 963-964
- site boundaries, 153-155
- software sources, 185
- SSL, 136-137
- System Center Essentials on single server, 924-928
- VMM library, 668-669
- WebDAV, 137-138
- Windows Management Pack, 415
- Connector Framework, 277-278, 711**
- connectors (Service Manager)**
 - Configuration Manager connector deployment, 752-753
 - deployment
 - Active Directory connector, 747-748
 - Operations Manager connector, 748-752
- consoles. *See specific consoles***
- consolidated reporting, 34**
- containers**
 - Discovered Inventory, 960
 - System Management container, creating with ADSI Edit, 134-135
 - Update Repository, 59

- content, locating with clients, 174-176**
- content distribution**
 - operating system deployment, 59-60
 - software distribution, 58
 - software update distribution, 59
- Continuous Data Protection (CDP), 547-548**
- Conversion Information page (Convert Physical Server Wizard), 677**
- Convert Physical Server Wizard, 673-679**
 - Additional Properties page, 677
 - Conversion Information page, 677
 - Gather System Information page, 674-675
 - Select Networks page, 677
 - Select Path page, 676
 - Select Source page, 674, 676
 - Summary page, 678-679
 - Virtual Machine Identity page, 674
 - Volume Configuration page, 675-676
- Convert Virtual Server Wizard, 679-683**
 - Additional Properties page, 682
 - Select Host page, 681-682
 - Select Networks page, 682
 - Select Path page, 682
 - Summary page, 682-683
 - Virtual Machine Identity page, 680-681
- converting servers to virtual guest sessions, 967-968**
- core client access licenses, 47**
- Create New Protection Group Wizard, 570-574, 589-592, 616-617**
- Create User Role Wizard, 687-690**
- CreatingCustomReportsByUsingSQLViews.msi, 229**
- Critical alerts, 365**
- critical events, resolving, 942-944**
- CRL Distribution Point (CDP) settings, 119-120**
- Cross Platform Management Packs**
 - configuring, 461-465
 - explained, 461
 - reports, 467-468
 - views, 465-466
- current usage analysis, 39**
- custom ACS (Audit Collection Services) reports, 525-528**

- custom AI (Asset Intelligence) catalogs, 245-246
- custom collections, creating, 182-185
- custom host ratings (VMs), 693-695
- custom management packs, 288
 - Authoring Console, 481
 - creating, 481-485
 - editing existing XML management pack files, 485-486
 - sealing management packs via command line, 486
- custom operating system images, 213-214
- custom reports, 231
- custom volumes (DPM), 579-580
- Customization tab (Computer Client Agent), 179

D

- D2D (disk-to-disk), 546
- D2D2T (disk-to-disk-to-tape), 546
- DA (Distributed Application) object, 486-487
- Daily Alert report, 513, 519-521
- DAS (Direct Attached Storage), 98-100, 297-299, 717
- Dashboard view (Operations Manager console), 390
- dashboards. *See* SLDs (Service Level Dashboards)
- data flow, 97-98
- Data Protection Manager. *See* DPM (Data Protection Manager) 2010
- data recovery, DPM (Data Protection Manager) 2010, 580-581
- data warehouse (Service Manager), 711, 738-741
- Data Warehouse Write Action account, 282
- Database Engine Health view, 458
- Database Free Space view, 458
- Database Grooming settings (OpsMgr), 360-361
- database server (VMM), designing, 648
- Database State view, 450, 457
- databases
 - audit collection database, 275-276, 287
 - CMDB (configuration management database), 711
 - Configuration Manager databases, 219-220
 - Database Grooming settings, 360-361
 - Exchange databases
 - protecting, 589-592
 - restoring, 592-594
 - integrated solutions databases, 19
 - master database, 287
 - operations database, 296
 - Operations Manager database, 287
 - backing up, 379-384
 - explained, 268-269
 - hardware/software requirements, 268-269
 - recovering, 611
 - Reporting data warehouse, 269-270
 - reporting database, 296
 - Service Manager database, backing up, 754-756
 - Site Server databases, 69-70
 - sizing, 89-90, 292-294
 - SQL Server databases
 - protecting, 598-600
 - restoring, 600-602
 - SQL End User Recovery, 602-605
 - VMM database
 - deployment, 650
 - designing, 648
- dataldr.log file, 242
- DB Space Free (%) monitor, 456
- DC Active Alerts view, 432
- DC Events view, 433
- DC Performance Data view, 433
- DC Server 2008 Active Alerts view, 433
- DC Server 2008 Events view, 433
- DC Server 2008 State view, 433
- DC State view, 433
- DCDIAG task, 436

DCM (Desired Configuration Management)

applying baselines to collections, 251-252

Client Agent, 247-248

defining configuration baselines, 251

defining configuration items to monitor, 248-251

explained, 63, 247-248

monitoring baselines and compliance, 246-253

deadlines, setting on updates, 956-957

declining updates, 954-956

Default Management Point, 174

defragmentation applications, file exclusions for, 376-377

Delegated Administrator role (VMM), 684, 686-687

Delete Aged Client Access License Data Properties task, 242

deleting CIs (configuration items), 836-838

delivering

reports

Alert reports, 507-508

Performance reports, 502-503

delivering reports, 496-497

Deploy Virtual Machine Wizard, 695-697

deployment

Central Sites. *See* Central Sites

certificates

Certificate Auto-Enrollment GPO, 120-122

Document Signing Certificate, 126

explained, 120

OS Deployment certificate, 124

publishing certificate templates, 126-127

Server Authentication certificate templates, 124-126

child Primary Sites, 148

Distribution Points, 155

DPM (Data Protection Manager) 2010

DPM server design, 558-559

DPM server preparation, 559-560

environment concerns, 553-554

explained, 552

project scope, 554

protection agents, 565-570

protection groups, 555-557

remote SQL instance, 560

running DPM installation, 560-562

storage requirements, 557-558

Enterprise Root CA, 118-120

FSP (Fallback Status Point), 151

operating systems

common scenarios, 204-205

common technologies, 59-60

creating software packages, 206-207

custom operating system images, 213-214

deployment technologies, 203-204

explained, 10, 203

monitoring, 213

requirements, 205

software distribution packages, 206

troubleshooting, 212-213

unknown computer support, 210-212

OpsMgr

design and planning phase, 313-315

design principles training, 313

explained, 312-313

pilot phase, 317-319

POC (proof of concept) phase, 315-317

production phase, 319

time estimates per phase, 319

regional site components, 161-162

RP (Reporting Point), 151-152

RSP (Reporting Service Point), 152-153

Service Manager

Active Directory connector, 747-748

components, 735-738

Configuration Manager connectors, 752-753

data warehouse, 738-741

Design and Planning phase, 728-730

Design Principles Training phase, 728

Extract, Transform, and Load (ETL) jobs, 743-744

management group registration, 741-743

- Operations Manager connector, 748-752
- Pilot phase, 732-734
- POC (proof of concept) phase, 730-732
- Production phase, 734
- steps, 734-735
- time estimates per phase, 734-735
- Web Portals, 744-746
- Site System roles, 149-150
- SLP (Server Locator Point), 150-151
- software. *See* software distribution
- VMM (Virtual Machine Manager)
 - Administrator Console, 654-656
 - Agent, 657-661
 - multiple-server deployment, 650
 - Self-Service Portal, 656-657
 - single-server deployment, 650
 - understanding environment, 644-649
 - VMM Server, 649-654
- VMs (virtual machines), 695-697
- WDS (Windows Deployment Service), 161
- deployment templates, 59, 196-197**
- deprovisioning process, managing, 867-868**
- Design and Planning phase**
 - OpsMgr deployment, 313-315
 - Service Manager deployment, 728-730
- Design Principles Training phase**
 - OpsMgr deployment, 313
 - Service Manager deployment, 728
- designing**
 - ConfigMgr architecture
 - bandwidth control, 93-94
 - boundaries, 94-96
 - client discovery and deployment, 91
 - client settings, 96-97
 - collections, 90-91
 - data flow, 97-98
 - disk performance, 98
 - explained, 107
 - large enterprise, 108-109
 - multiple sites, 92
 - PXE Service Points (PSPs), 94
 - SAN versus DAS, 98-100

- site-specific configuration settings, 92-93
 - small and medium enterprise, 107
 - SQL versions, 100-101
 - State Migration Points (SMPs), 94
 - user/group discovery, 91-92
- DPM (Data Protection Manager) server, 558-559
- MDM (Mobile Device Manager) implementation
 - medium to large environment with extensive enrollment requirements, 874-875
 - small environment with advanced IPsec VPN security requirements, 873
 - small environment with basic SSL security requirements, 872
- OpsMgr implementation
 - large enterprise design, 308-312
 - medium enterprise design, 305-308
 - small enterprise design, 303-305
- Service Manager architecture
 - explained, 719
 - large enterprise design, 724-726
 - medium enterprise design, 722-724
 - small enterprise design, 720-722
- Desired Configuration Management. *See* DCM (Desired Configuration Management)**
- Desired Configuration Management Client Agent, 96**
- device discovery. *See* discovery**
- Device Encryption Enabled setting (Exchange Server 2007), 906**
- Device Management server**
 - explained, 870-871
 - prerequisites, 875
- device monitoring (SNMP)**
 - explained, 489-490
 - troubleshooting, 490-491
- Device Status Details report, 898**
- Device Status Summary report, 898**
- devices**
 - adding/modifying with Capacity Planner Hardware Editor, 852
 - blocking device connections, 892-893

device groups

- approving packages to be deployed to device groups, 897-898

- creating with Model Wizard, 896-897

- device inventory and tracking, 41

- device provisioning, 41, 886-887

- device wipe and deprovisioning, 41

- disabling applications on, 901-902

discovery

- autodiscover, 938-939

- manual discovery, 940-941

- enforcing policies to, 866-867, 902

- identifying devices that are pending enrollment, 888-889

- locking down, 901

- managing with MDM (Mobile Device Manager), 866

- Mobile VPN connections, 904

- mobility access controls, 903-904

- pre-enrolling, 887-888

- setting password policies for, 902-903

- tracking, 867

- wiping, 890-892

DFS namespace, protecting data in, 585

Diagram view (Operations Manager console), 390

“dip stick” health checks, 368-369

Direct Attached Storage (DAS), 98-100, 297-299, 717

Disable Audit Collection task, 413

Disable-NotificationSubscription cmdlet, 394

disabling applications, 901-902

disaster recovery**backups**

- ConfigMgr, 85-86

- OpsMgr, 287-289

- defined, 283

Discovered Inventory container, 960

discovery

- autodiscover, 938-939

- discovery methods, 164-165

- explained, 937-938

- manually discovering computers, 939-940

- manually discovering network devices, 940-941

disk performance

- ConfigMgr, 98

- OpsMgr, 296-297

- Service Manager, 717

disk-based storage, 546

disks, adding to storage pool, 563-564

disk-to-disk (D2D), 546

disk-to-disk-to-tape (D2D2T), 546

Display Account Settings task, 420

Display Active Connections task, 420

Display Active Sessions task, 420

Display Local Users task, 420

Display Network Shares task, 420

Display Server Statistics task, 420

Display Workstation Statistics task, 420

Distributed Application (DA) object, 486-487

distributed application monitoring

- building distributed application model, 487-488

- explained, 486-487

- sample distributed applications, 488-489

distributing software. See software distribution

Distribution Points, 115

- BITS-enabled Distribution Points, 73

- Branch Distribution Points, 73

- BranchCache, 74

- deployment, 155

- explained, 72-73, 174, 181-182

- Protected Distribution Points, 74

- selecting, 190-191

- Standard (SMB) Distribution Points, 73

Distributor State view, 458

DMZ servers

- monitoring with certificates

- configuring agents to use certificates, 358

- creating certificate templates, 353

- explained, 352-353

- installing agents on DMZ servers, 356-357

- requesting certificates from root CA for mutual authentication, 355-356

- requesting root CA certificates, 353-355

- securing with certificates, 283

Document Signing Certificate

- explained, 103, 115

- requesting, 140-143

domain controller performance collection, 431-433**Domain Join accounts, 84****domain-attached systems, installing agents on, 973-974****downloading management packs (OpsMgr), 401-402****DPM (Data Protection Manager) 2010**

- Administrator Console, 575-577

- business solutions addressed by, 23-24

- capabilities, 24-27

- CDP (Continuous Data Protection), 547-548

- cloud-based storage, 547

- configuring

- disks, 563-564

- protection agent deployment, 565-570

- protection groups, 570-574

- tape library, 564-565

- console, 23

- custom volumes, 579-580

- D2D2T (disk-to-disk-to-tape), 546

- data recovery, 580-581

- deployment

- DPM server design, 558-559

- DPM server preparation, 559-560

- environment concerns, 553-554

- explained, 553

- project scope, 554

- protection agents, 565-570

- protection groups, 555-557

- remote SQL instance, 560

- running DPM installation, 560-562

- storage requirements, 557-558

- disk-based storage, 546

- Exchange Server protection

- additional considerations, 597-598

- high-availability considerations, 596-597

- protecting Exchange databases, 589-592

- recoverable, 588-589

- restoring Exchange databases, 592-594

- restoring mailboxes, 594-596

- explained, 7, 22, 542-544, 582-583

- file server protection

- data in DFS namespaces, 585

- data on file server clusters, 586

- data on mount points, 586

- data sources and recoverable data, 584-585

- hardware requirements, 552

- history and revisions, 27

- DPM 2006, 548

- DPM 2006 SP1, 548-549

- DPM 2007, 549-550

- DPM 2007 SP1, 550

- DPM 2010, 550-552

- installation, 560-562

- integrating with Operations Manager, 620-624

- Management Shell, 577-578

- modern data recovery needs, 544-545

- protection groups

- creating, 570-574

- designing, 555-557

- SharePoint farm protection

- data sources and recoverable data, 605

- preparing SharePoint for protection, 606-607

- protecting SharePoint farms, 607-609

- recovering content databases, 611

- recovering SharePoint farms, 609-611

- recovering sites, lists, and items, 611-615

- software requirements, 552-553

- SQL Server protection

- EUR Client, 603-604

- explained, 598

- protecting SQL Server databases, 598-600

- restoring SQL Server databases, 600-602

- SQL End User Recovery feature, 602-605

- System State protection, 586-587

- virtualized environment protection
 - automatically protecting new machines, 617-618
 - explained, 615
 - ILR (item-level recovery), 620-619
 - protecting Hyper-V virtual machines, 615-617
 - recovering Hyper-V virtual machines, 618-619

DPM Setup Wizard, 561-562

DPMRecoveryWebApplication, 606-607

dragging and dropping VM onto host server, 704

drivers, managing, 208

E

Edge Servers Alerts view, 449

Edge Servers State view, 449

editing

- capacity models, 860-862
- configuration.mof file, 225-226
- sms_def.mof, 226
- XML management pack files, 485-486

editors

- Capacity Planner Hardware Editor, 847
- Capacity Planner Model Editor, 847
- Hardware Editor
 - adding/modifying computers, 852
 - adding/modifying devices, 852
 - explained, 851-852
 - list icons, 852
- Model Editor, 860-862

email

- creating incidents from, 782-783
- email host server addresses, changing, 979
- inbound email settings, 766-769

Enable Audit Collection task, 407

Enable-NotificationSubscription cmdlet, 394

enabling. See configuring

encryption keys, backing up, 756

end-to-end service monitoring, 259

enforcing policies to mobile devices, 866-867, 902

Enrollment server

- explained, 871
- installing, 880
- prerequisites, 876

Enterprise Edition (SQL Server), 100

Enterprise Root CA, 103, 115

- deployment, 118-120
- validating, 120

Enumerate Trusts task, 436

ETL (Extract, Transform, and Load) jobs, 743-744

EUR Client, 603-604

evaluating incidents, 783-784

Event view (Operations Manager console), 389

events

- critical events, resolving, 942-944
- event correlation, 17
- event log collection, 17
- warning events, 944-945

ExBPA Events view, 447

Exchange 2007 Management Pack

- Client Access Server Monitoring, 445-447
- configuring, 438-442
- explained, 433
- Internet mail flow, 443-444
- intraorganization synthetic transactions, 443-444
- reports, 453-454
- tasks, 452-453
- views, 447-452

Exchange Server

- and MDM (Mobile Device Manager), 904-908
- protecting with DPM (Data Protection Manager)
 - additional considerations, 597-598
 - high-availability considerations, 596-597
 - protecting Exchange databases, 589-592
 - recoverable, 588-589
 - restoring Exchange databases, 592-594
 - restoring mailboxes, 594-596

exporting

- management packs, 403-404
- reports from OpsMgr, 496

Export-MDMGatewayConfig command, 882

EXTADSch.exe, 133-134

ExtADSch.log file, 134

extending AD (Active Directory) schema, 56-57, 133-134

Extract, Transform, and Load (ETL) jobs, 743-744

F

Fallback Status Point (FSP), 74, 114

fault tolerance

- clustering, 285-286
- defined, 283
- explained, 84-85, 284-285
- management group redundancy, 284
- NLB (Network Load Balancing), 85

file exclusions for antivirus and defragmentation applications, 376-377

file servers

- clusters, protecting data on, 585
- protecting with DPM (Data Protection Manager)
 - data in DFS namespaces, 585
 - data on file server clusters, 585
 - data on mount points, 586
 - recoverable, 584-585

files

- AIUpdateSvc.log, 236
- ccm.log, 166
- CCR (Client Configuration Request) files, 167
- configuration.mof file, editing, 225-226, 241-242
- dataldr.log, 242
- ExtADSch.log file, 134
- file attachment limits, 761-762, 794, 812-813
- fspmgr.log, 151, 166
- fspMSI.log, 151

IDMIF files, 221

InventoryAgent.log, 220

NOIDMIF files, 221

ReportingServicesService.exe.config, 512-513

Rsetup.log, 151-152

sms_def.mof, editing, 226

SMSFSPSetup.log, 151

SMSReportingInstall.log, 151-152

SNK (Strong Name Key) files, 486

SUPSetup.log, 159

WSUSCtrl.log, 159

Firewall Rule exceptions, 978-979

firewalls

- configuring for SQL Server, 132-133
- Firewall Rule exceptions, 978-979
- OpsMgr communication ports, 280-281

Flush Health Service State and Cache task, 413

folders

- All Open Unassigned Incidents, 784
- My Incidents, 785
- Software Updates - A Compliance folder, 202

Forensic reports, 523

FSP (Fallback Status Point), 74, 114, 151

fspmgr.log file, 151, 166

fspMSI.log file, 151

G

Gateway server

- explained, 273-274, 871
- hardware/software requirements, 274
- installing, 880-884
- prerequisites, 876

Gather System Information page (Convert Physical Server Wizard), 674-675

General tab (Computer Client Agent), 178

geographic-based management groups, 301-302

Get-Command command, 671

Get-Help cmdlet, 578

Get-Help command, 671

Get-NotificationSubscription cmdlet, 394-395

Get-NotificationSubscriptions cmdlet, 394

Global Configuration Setting (2005/2008) task, 459

Global Management Group Settings (OpsMgr), 359-361

Global Topology view (Model Editor), 860-861

GP Update task, 436

Group Policy templates, installing, 898-900

groups

adding users to, 541

creating for SLD sites, 540

device groups

approving packages to be deployed to device groups, 897-898

creating with Model Wizard, 896-897

discovery, 91-92

group policies

Certificate Auto-Enrollment GPO, 120-122

Group Policy templates, installing, 898-900

in MDM (Mobile Device Manager), 871-872

host groups

creating, 666-667

dragging and dropping VMs onto, 705

management groups

defining, 295

geographic-based management groups, 301-302

Global Management Group Settings, 359-361

multiple management groups, 301

political or security-based management groups, 302

redundancy, 284

registering, 741-743

protection groups

creating, 570-574

designing, 555-557

H

Hardware 03A-10C reporting classes, 237-238

Hardware Editor

adding/modifying computers, 852

adding/modifying devices, 852

explained, 847, 851-852

list icons, 852

hardware inventory

customizing

creating Registry keys on client, 223-224

editing configuration.mof file, 225-226

editing sms_def.mof file, 226

explained, 223

explained, 61-62

viewing, 960

Hardware Inventory Client Agent, 96, 222-223

Hardware page (Model Wizard), 857-858

hardware reports (AI), 247

hardware requirements

for ConfigMgr, 86-87

for DPM (Data Protection Manager), 552

for OpsMgr, 290

ACS (Audit Collection Services), 277

audit collection database, 276

audit collector, 275

Connector Framework, 278

Gateway server, 274

management server, 267

Operations Console, 271

Operations Manager database, 268

Reporting data warehouse, 270

Reporting Server, 270

Root Management Server, 266

Web console, 272

for SCCP (System Center Capacity Planner), 848-849

for Service Manager, 714-715

for System Center Essentials

multiserver configuration, 918

multisite configuration, 919

single-server configuration, 918

for VMM (Virtual Machine Manager)

Administrator Console, 642

Self-Service Portal, 643

VMM server, 640

Health Service Heartbeat Failure monitor, 409

Health Service tasks, 412-414

Health Service Watcher, 363

Health Validator Point, 74-75

high-availability scenarios and DPM (Data Protection Manager), 596-597

holding change requests, 825-826

hosts

dragging and dropping VMs onto, 704

host clusters, 667-668

host groups

creating, 666-667

dragging and dropping VMs onto, 705

host ratings, customizing for VMs (virtual machines), 693-695

managing, 667-668

virtual host management, 44-45

Hub Server Alerts view, 449

Hub Server State view, 449

Hyper-V host servers

adding, 965

automatically protecting new machines, 617-618

host clusters, 667-668

host groups, creating, 666-667

importing VMware guest sessions to, 968-969

managing, 667-668

protecting, 615-617

recovering, 618-619

virtual network switches, creating, 980

VMM (Virtual Machine Manager). See VMM (Virtual Machine Manager)

explained, 105

requirements and limitations, 105-106

site system placement, 106-107

icons, Hardware Editor list icons, 852

IDMIF files, 221

IIS (Internet Information Services), 287

IIS 6.0 metabase backup, 383-384

IIS 7.x configuration backup, 385

implementing, 134-135

SSL configuration, 136-137

WebDAV, 137-138

ILR (item-level recovery), 620-619

images, 852

importing

management packs, 369-371

management packs (OpsMgr), 400

software licensing data, 243-245

inbound email settings, 766-769

Incident Analyst report, 800, 803

Incident Detail report, 800

Incident KPI Trend report, 800

incident management

announcements, publishing, 787-788

creating with OpsMgr alerts, 777-780

explained, 34-35, 757-760

incident settings, 761

file attachment limits, 761-762

inbound email settings, 766-769

incident prefix, 761

Operations Manager Web console settings, 765-766

priority calculation, 762-764

resolution times, 764-765

incidents

analyzing, 784-787

creating from emails, 782-783

creating manually, 775-777

creating with Self-Service Web Portal, 779-781

defined, 760

evaluating and assigning, 783-784

resolving, 791-793

IBCM (Internet-Based Client Management)

client site assignment, 107

configuring, 156-157

notifications

explained, 770

Service Manager notification architecture, 770-771

SMTP notification channel, 771-772

subscriptions, 773-775

templates, 772-773

problem settings

explained, 793

file attachment limits, 794

priority calculation, 795-796

problem prefix, 793

problems

analyzing, 797-798

creating, 796-797

defined, 760, 796

resolving, 799

reports

explained, 799

Incident Management Report Library, 800-804

Problem Management Report Library, 804-805

Service Manager report controls, 799-800

troubleshooting tasks, 788-791

Incident Management Report Library, 800-804

Incident Resolution report, 803-804

incidents. *See also* incident management

analyzing, 784-787

creating

from emails, 782-783

manually, 775-777

with OpsMgr alerts, 777-780

with Self-Service Portal, 779-781

creating change requests from, 819

evaluating and assigning, 783-784

resolving, 791-793

troubleshooting, 788-791

Information alerts, 365

installing

Administrator Console (VMM), 654-656

agents, 166-167

on DMZ servers, 356-357

on domain-attached systems, 973-974

Firewall Rule exceptions, 978-979

on nondomain joined systems, 974-977

Central Site Server, 143-145

Configuration Manager 2007 R2 upgrade, 147

DPM (Data Protection Manager) 2010, 560-562

FSP (Fallback Status Point), 151

Group Policy templates, 898-900

management packs (OpsMgr), 402-403

MDM (Mobile Device Manager)

Administrator Tools, 885-886

Enrollment server, 880

Gateway server, 880-884

initial MDM acquisition and setup options, 877-879

Self-Service Portal, 884-885

step-by-step installation process, 879-880

OpsMgr

explained, 321-324

multiserver OpsMgr 2007 R2 install, 329-337

OpsMgr 2007 R2 ACS (Audit Collection Services) install, 337-343

single-server OpsMgr 2007 R2 install, 324-329

UNIX/Linux agents, 349-352

Windows agent installation, 343-345

RP (Reporting Point), 151-152

RSP (Reporting Service Point), 152-153

SCCP (System Center Capacity Planner), 849-850

Self-Service Portal (VMM), 656-657

SLDs (Service Level Dashboards), 537-539

SLP (Server Locator Point), 150-151

SQL Server, 130-132

System Center Essentials on separate servers

management console tools, 928-929

SCE Reporting Services, 929-930

- System Center Essentials on single server preparation, 920
- running SCE Configuration Wizard, 924-928
- running SCE installation, 921-923
- VMM Agent, 657-661
- VMM Server, 651-692
- Web Portals, 744-746
- WSUS 3.0 SP2, 138-139

integrated solutions databases, 19

Internet

- downloading management packs from, 401-402
- importing management packs from, 400

Internet Client, 11

Internet Information Services. *See* IIS (Internet Information Services)

Internet mail flow, configuring, 443-444

Internet Management Point, 174

Internet-Based Client Management. *See* IBCM (Internet-Based Client Management)

Intersite Replication Traffic view, 435

intraorganization synthetic transactions, configuring, 443-444

inventory

- collecting manually, 960-961
- configuring Client Agents for
 - explained, 221-222
 - Hardware Inventory Client Agent, 222-223
 - Software Inventory Client Agent, 222
- customizing hardware inventory
 - creating Registry keys on client, 223-224
 - editing configuraton.mof file, 225-226
 - editing sms_def.mof file, 226
 - explained, 223
- of devices, 41
- explained, 61-62, 960
- IDMIF files, 221
- inventory collection process, 220
- NOIDMIF files, 221
- validating inventory data, 227
- viewing, 228, 960

InventoryAgent.log file, 220

investigating change requests, 822-824

Ipconfig task, 420

item-level recovery (ILR), 620

J-K

Jobs dialog box, 703

KB (knowledge base), 711

knowledge base (KB), 711

L

large enterprise design

- ConfigMgr, 108-109
- OpsMgr, 308-312
- Service Manager, 724-726

LDP Tool Console Task, 436

legacy reports, 231

libraries

- Activity Management Report Library, 841
- Change Management Report Library, 840-841
- Configuration Management Report Library, 842-843
- Incident Management Report Library, 800-804
- Problem Management Report Library, 800-804
- tape libraries, configuring, 564-565
- VMM library
 - configuring, 668-669
 - designing, 643-649
 - explained, 632-633

License 01A-15B reporting classes, 238-239

licensing

- CAL license tracking, 241-242
- core client access licenses, 47
- explained, 46

- license reports (AI), 247
- Server Management Suite licenses, 47
- software licensing data, importing, 243-245
- Linux agents, installing, 349-352**
- Linux Non-Privileged Users, assigning to UNIX Action Account profile, 464**
- Linux Privileged Users, assigning to UNIX Privileged Account profile, 464-465**
- List of Activities report, 841**
- List of Incidents report, 801-802**
- List of Manual Activities report, 841**
- List of Problems report, 804-806**
- List of Review Activities report, 841**
- List of RFCs report, 840**
- List Processes task, 420**
- List Services task, 420**
- List Top Processes on DC task, 436**
- Local Administrator account, 282**
- Local Latency view, 450**
- locking devices, 901**
- log files**
 - AIUpdateSvc.log, 236
 - ccm.log, 166
 - dataldr.log, 242
 - ExtADSch.log file, 134
 - fspmgr.log, 166
 - fspmgr.log file, 151
 - fspMSI.log, 151
 - InventoryAgent.log, 220
 - Rsetup.log, 151-152
 - SMSFSPSetup.log, 151
 - SMSReportingInstall.log, 151-152
 - SUPSetup.log, 159
 - WSUSCtrl.log, 159
- Logical Disk Defragmentation, 420**
- Logical Disk Free Space monitor, 416**
- Logical Disk State view, 466**
- logon auditing, 242-243**

M

- Mail Flow State view, 450**
- Mailbox Servers Active Alerts view, 449**

- Mailbox Servers State view, 450**
- Mailbox Sites page (Model Wizard), 853-854**
- mailboxes**
 - monitor and rule sync times, 442
 - restoring, 594-596
- Maintenance mode**
 - putting servers into, 945-947
 - in VMM 2008 R2, 639
- maintenance windows for collections, 184**
- Management Configuration Service - Windows Service State monitor, 409-410**
- management console (MDM), 870**
- management console (SCE)**
 - Administration option, 935-937
 - Authoring option, 937
 - Computers option, 931
 - explained, 930-931
 - installing console tools, 928-929
 - Monitoring option, 932-933
 - Reporting option, 934-935
 - Software option, 933-934
 - Updates option, 933-934
- management groups**
 - defining, 295
 - geographic-based management groups, 301-302
 - Global Management Group Settings, 359-361
 - multiple management groups, 301
 - political or security-based management groups, 302
 - redundancy, 284
 - registering, 741-743
- Management Information Format (MIF) files**
 - IDMIF files, 221
 - NOIDMIF files, 221
- Management Pack Templates**
 - explained, 468-469
 - OLE DB Data Source Template, 474-476
 - Process Monitoring Template, 476-478
 - TCP Port Template, 477-479
 - Unix/Linux Log File Template, 478-479
 - Unix/Linux Service Template, 480
 - Web Application Template, 469-471
 - Windows Service Template, 471-474

management packs

- Active Directory Management Pack
 - client monitoring, 426-427
 - configuring, 423-424
 - domain controller performance collection, 431-433
 - explained, 423
 - replication monitoring, 427-431
 - reports, 437-438
 - tasks, 436-437
 - views, 432-436
- alert tuning, 405-408
- Cross Platform Management Packs
 - configuring, 461-465
 - explained, 461
 - reports, 467-468
 - views, 465-466
- custom management packs, 288
 - Authoring Console, 481
 - creating, 481-485
 - editing existing XML management pack files, 485-486
 - sealing management packs via command line, 486
- downloading, 401-402
- Exchange 2007 Management Pack
 - Client Access Server Monitoring, 445-447
 - configuring, 438-442
 - explained, 433
 - Internet mail flow, 443-444
 - intraorganization synthetic transactions, 443-444
 - reports, 453-454
 - tasks, 452-453
 - views, 447-452
- explained, 258, 386-388
- exporting, 403-404
- importing, 369-371, 400
- installing manually, 402-403
- Management Pack Templates
 - explained, 468-469
 - OLE DB Data Source Template, 474-476

- Process Monitoring Template, 476-478
- TCP Port Template, 477-479
- Unix/Linux Log File Template, 478-479
- Unix/Linux Service Template, 480
- Web Application Template, 469-471
- Windows Service Template, 471-474
- Management Pack tree item, 393, 399-400
- Operations Manager Management Pack
 - configuring, 408-410
 - explained, 420-408
 - tasks, 412-414
 - views, 410-412
- override management packs, 287, 404-405
- SQL Server Management Pack
 - configuring, 455
 - explained, 454-455
 - reports, 460-461
 - tasks, 459-460
 - tuning, 455-457
 - views, 457-459
- updating, 371-372
- Windows Management Pack
 - configuring, 415
 - explained, 415
 - reports, 421-423
 - tasks, 418-421
 - tuning, 416
 - views, 416-419
- Management Packs tree item (OpsMgr), 393, 399-400
- management points. *See specific management points*
- Management Server
 - explained, 266-268
 - hardware/software requirements, 267-268
 - Management Server Action account, 282
- Management Shell (DPM), 577-578
- manual activities (MAs), 831-832
- Manual Activity Details report, 841
- manual agents, accepting, 359-360
- MAs (manual activities), 831-832
- master database, 287

Maximum Attachment Size setting (Exchange Server 2007), 907

Maximum Calendar Age setting (Exchange Server 2007), 907

Maximum E-mail Age Filter setting (Exchange Server 2007), 907

Maximum E-mail Body Truncation Size setting (Exchange Server 2007), 907

Maximum Failed Password Attempts setting (Exchange Server 2007), 907

Maximum HTML E-mail Body Truncation Size setting (Exchange Server 2007), 907

Maximum Inactivity Time Lock setting (Exchange Server 2007), 907

MDM (Mobile Device Manager)

active updates and device management, 41

business solutions addressed by, 40-41

capabilities, 864-868

help desk tools, 867-868

mobile device management, 866

mobile device tracking, 867

policy enforcement, 866-867

provisioning and deprovisioning management, 867-868

console, 40

designing implementation of

medium to large environment with extensive enrollment requirements, 874-875

small environment with advanced IPSec VPN security requirements, 873

small environment with basic SSL security requirements, 872

devices

approving packages to be deployed to device groups, 897-898

blocking device connections, 892-893

creating device groups, 896-897

device provisioning, 41

disabling applications on, 901-902

enforcing policies to, 902

identifying devices that are pending enrollment, 888-889

inventory and tracking, 41

locking down, 901

pre-enrolling, 887-888

provisioning through Self-Service Portal, 886-887

setting password policies for, 902-903

wipe and deprovisioning, 41

wiping, 890-892

explained, 8, 40

Group Policy templates, installing, 898-900

history and revisions, 42, 868

initial release of MDM 2008, 868

MDM 2008 SP1, 868-870

installing

Administrator Tools, 885-886

Enrollment server, 880

Gateway server, 880-884

initial MDM acquisition and setup options, 877-879

Self-Service Portal, 884-885

step-by-step installation process, 879-880

and Microsoft Exchange Server, 904-908

Mobile VPN connections, 904

mobility access controls, 903-904

packages

approving packages to be deployed to device groups, 897-898

checking status of, 898

password and PIN control, 41

preparing server for, 877

prerequisites

for MDM Device Management Server, 875

for MDM Enrollment server, 876

for MDM Gateway server, 876

for SQL Database Server component, 875-876

reports, 898

resetting passwords with, 889-890

and SCCM (System Center Configuration Manager) 2007, 908-909

self-service management, 41-42

Self-Service Portal

device provisioning through, 886-887

installing, 884-885

server roles

- Active Directory and group policies, 871-872
- Device Management server, 870-871
- Enrollment server, 871
- explained, 870
- Gateway server, 871
- management console, 870
- SQL Server, 871

software packaging, 894-896

MDT (Microsoft Deployment Toolkit), 60

medium enterprise design

- ConfigMgr, 107
- OpsMgr, 305-308
- Service Manager, 722-724

Memory Pool Non-Paged Bytes rule, 416

Memory Pool Paged Bytes rule, 416

metering. See software metering

Microsoft Deployment Toolkit (MDT), 60

Microsoft Exchange Server and MDM (Mobile Device Manager), 904-908

Microsoft Operations Manager (MOM) 2000, 20

Microsoft Operations Manager (MOM) 2005, 20

MIF (Management Information Format) files

- IDMIF files, 221
- NOIDMIF files, 221

Migrate Storage action (VMM), 702-703

Migrate Virtual Machine Wizard, 701-702

migrating VMs (virtual machines), 699-705

- dragging and dropping VM onto host group, 705
- dragging and dropping VM onto host server, 704
- Migrate Storage action, 702-703
- Migrate Virtual Machine Wizard, 701-702
- supported storage migration technologies, 701
- supported virtual machine migration technologies, 700-706

Minimum Device Password Complex Characters setting (Exchange Server 2007), 907

Minimum Password Length setting (Exchange Server 2007), 907

Mixed mode security (ConfigMgr), 79-80

Mobile Device Client Agent, 96

Mobile Device Management features (ConfigMgr), 78-79

Mobile Device Manager. See MDM (Mobile Device Manager)

mobile devices. See devices

Mobile VPN connections, creating, 904

mobility access controls, 903-904

Model Editor, 847, 860-862

Model Summary page (Model Wizard), 859-860

Model Wizard

- Application page, 858-859
- Client-Only Sites page, 854-855
- explained, 853
- Hardware page, 857-858
- Mailbox Sites page, 853-854
- Model Summary page, 859-860
- Networks page, 855-856
- starting, 853

Model Wizard (Capacity Planner), 847

models. See capacity models

modifying

- devices with Capacity Planner Hardware Editor, 852
- VMM (Virtual Machine Manager) user roles, 690-691

MOM (Microsoft Operations Manager) 2000, 20

MOM (Microsoft Operations Manager) 2005, 20

monitoring

- Active Directory clients, 426-427
- Active Directory replication monitoring, 427-431
- applications, 17-18
- automatic client installation, 167
- baselines and compliance, 246-253
- clients, 17
- distributed application monitoring
 - building distributed application model, 487-488
 - explained, 486-487
 - sample distributed applications, 488-489

- DMZ servers with certificates
 - configuring agents to use certificates, 358
 - creating certificate templates, 353
 - explained, 352-353
 - installing agents on DMZ servers, 356-357
 - requesting certificates from root CA for mutual authentication, 355-356
 - requesting root CA certificates, 353-355
- end-to-end service monitoring, 259
- network monitoring, 352
- nondomain member considerations, 294-295
- operating system deployment, 213
- performance, 395-399
- servers, 17, 44
- SNMP device monitoring
 - explained, 489-490
 - troubleshooting, 490-491
- software deployment, 195
- software update deployment, 202-203
- with System Center Essentials
 - alerts, 942
 - checking health of servers, 945
 - explained, 941-942
 - handling warning events, 944-945
 - putting servers in Maintenance mode, 945-947
 - resolving critical events, 942-944
- systems, 17-18
- with VMM (Virtual Machine Manager), 669
- websites
 - configuring response time alerts, 963-964
 - creating website monitoring agents, 961-963
- Monitoring option (SCE), 932-933**
- monitors, 258. *See also specific monitors***
- monthly administration tasks (SCE), 983-984**
- Most Common Alerts report, 513, 514-515**
- mount points, protecting data on, 586**
- MP (Management Point), 75**
- MPSEAL.EXE, 486**
- MSDB database, 287**

- multiple management groups, 301**
- multiple-server VMM deployment, 650**
- multiserver OpsMgr 2007 R2 install, 329-337**
- multisite Configuration Manager hierarchy, 92**
- My Incidents folder, 785**

N

- namespaces, DFS, 585**
- Native mode security (ConfigMgr)**
 - certificate requirements, 102
 - certificate templates, 103-104
 - explained, 79-80, 102
 - PKI (Public Key Infrastructure), 103
- NETDOM Query FSMO task, 436**
- NetIQ Enterprise Event Manager, 19-20**
- Network Access accounts, 84**
- network access, configuring, 178-181**
- Network Access Protection Client Agent, 73**
- Network Adapter State view, 466**
- network bandwidth requirements**
 - for ConfigMgr, 88-89
 - for OpsMgr, 291-293
- Network Load Balancing (NLB), 85**
- Networks page (Model Wizard), 855-856**
- New Package Wizard, 189**
- New Site Role wizard, 158-159**
- New-DeviceDiscoveryConfiguration cmdlet, 489**
- NLB (Network Load Balancing), 85**
- NLTEST task, 436**
- nodes, Watcher, 962-963**
- NOIDMIF files, 221**
- nondomain joined systems, installing agents on, 974-977**
- nondomain member considerations, monitoring, 294-295**
- Non-Privileged User accounts, configuring, 464**
- Not Connected errors, troubleshooting, 979-980**
- notifications**
 - automatic notifications of change request status, 833-834
 - configuring, 364-367

- explained, 260, 770
- OpsMgr administration, 393-395
- Service Manager notification architecture, 770-771
- SMTP notification channel, 771-772
- templates, 772-773
- tuning, 372-376

Notifications tree item (OpsMgr), 393-395

O

Object Identifiers (OIDs), 102, 118

Office Customization Wizard, 187-188

OIDs (Object Identifiers), 102, 118

OLE DB Data Source Template, 474-476

Operating System Performance view, 466

operating systems

- deployment, 10
 - common scenarios, 204-205
 - common technologies, 59-60
 - creating software packages, 206-207
 - custom operating system images, 213-214
 - deployment technologies, 203-204
 - explained, 203
 - monitoring, 213
 - OS install packages, 207-210
 - requirements, 205
 - software distribution packages, 206
 - troubleshooting, 212-213
 - unknown computer support, 210-212
- DPM (Data Protection Manager) 2010 support for, 552
- SCCP (System Center Capacity Planner) support for, 849
- supporting OS deployment, 160
- System Center Essentials support for, 915-916
- VMM support for
 - Administrator Console, 642
 - Self-Service Portal, 643
 - VMM Server, 641

operational data, processing with OpsMgr, 260

Operational Database Watchers Group to Management Group Availability Health Rollup Monitor, 409

Operations Console, 388-390

- explained, 259, 270-271
- hardware/software requirements, 271

operations database, 296

Operations Manager database

- backing up, 379-380
- explained, 268-269, 287
- hardware/software requirements, 268-269

Operations Manager Management Pack

- configuring, 408-410
- explained, 420-408
- tasks, 412-414
- views, 410-412

OperationsManagerAC database, 383-384

OperationsManagerDW database, 381-383

OpsMgr

- ACS (Audit Collection Services)
 - ACS Reporting, 276-277
 - audit collection database, 275-276
 - audit collector, 275
 - audit forwarder, 274
 - database, 287
- administration
 - daily tasks, 368-369
 - explained, 390
 - file exclusions for antivirus and defragmentation applications, 376-377
 - importing management packs, 369-371
 - management pack updates, 371-372
 - Management Packs tree item, 393, 399-400
 - notification and alert tuning, 372-376
 - Notifications tree item, 393-395
 - Pending Management tree item, 392-393
 - performance monitoring, 395-399
 - Web console performance view time frame, 377-378

agents

- configuring to use certificates, 358
- explained, 263-265
- installing on DMZ servers, 356-357
- UNIX/Linux agent installation, 349-352
- Windows agent installation, 343-345

alerts

- alert forwarder configuration, 346-349
- creating incidents with, 777-780
- explained, 259
- generating, 261
- tuning, 372-376

application monitoring, 17-18

backing up

- backup schedules, 378
- IIS 6.0 metabase backup, 384-385
- IIS 7.x configuration backup, 385
- OperationsManager database backup, 379-380
- OperationsManagerAC database backup, 383-384
- OperationsManagerDW database backup, 381-383
- RMS encryption key backup, 380-381

business solutions addressed by, 16

client system monitoring, 17

command shell, 272-273, 391-392

components summary, 262-263

configuring

- Agent Proxy configuration, 362-363
- agent restart recovery, 363-364
- Global Management Group Settings, 359-361
- notifications and subscriptions, 364-367

Connector Framework, 277-278

consoles

- explained, 259, 388
- operations console, 388-390
- Web console, 390-391

dashboards, 260

data storage

- disk performance, 296-297
- explained, 296

SAN versus DAS, 297-299

SQL versions, 299-301

databases

- ACS (Audit Collection Services), 287
- master database, 287
- MSDB database, 287
- operations database, 296
- Operations Manager database, 287
- reporting database, 296
- sizing, 292-294

disaster recovery

- backups, 287-289
- defined, 283

distributed application monitoring

- building distributed application model, 487-488
- explained, 486-487
- sample distributed applications, 488-489

DMZ servers, monitoring with certificates

- configuring agents to use certificates, 358
- installing agents on DMZ servers, 356-357
- requesting certificates from root CA for mutual authentication, 355-356
- requesting root CA certificates, 353-355

end-to-end service monitoring, 259

event correlation, 17

event log collection, 17

explained, 7, 15-16, 255-258

fault tolerance

- clustering, 285-286
- defined, 283
- explained, 284-285
- management group redundancy, 284

Gateway server

- explained, 273-274
- hardware/software requirements, 274

hardware requirements, 290

history and revisions, 19-20

IIS (Internet Information Services), 287

- installing
 - explained, 321-324
 - multiserver OpsMgr 2007 R2 install, 329-337
 - OpsMgr 2007 R2 ACS (Audit Collection Services) install, 337-343
 - single-server OpsMgr 2007 R2 install, 324-329
- integrated solutions databases, 19
- integrating with DPM (Data Protection Manager), 620-624
- integrating with VMM (Virtual Machine Manager), 646
- large enterprise design, 308-312
- management groups
 - defining, 295
 - geographic-based management groups, 301-302
 - multiple management groups, 301
 - political or security-based management groups, 302
- management packs. *See* management packs
- Management Server
 - explained, 266-268
 - hardware/software requirements, 267-268
- medium enterprise design, 305-308
- monitoring DMZ servers with, 352-353
- monitors, 258
- network bandwidth requirements, 291-293
- network monitoring, 352
- nondomain member considerations, monitoring, 294-295
- notifications
 - explained, 260
 - tuning, 372-376
- Operations Console
 - explained, 270-271
 - hardware/software requirements, 271
- Operations Manager connector, 748-752
- Operations Manager database, 268-269
- performance monitoring, 395-399
- phases of project deployment
 - design and planning, 313-315
 - design principles training, 313
 - explained, 312-313
 - pilot phase, 317-319
 - POC (proof of concept) phase, 315-317
 - production phase, 319
 - time estimates per phase, 320
- processing operational data, 260
- Reporting data warehouse
 - explained, 269-270
 - hardware/software requirements, 270
- Reporting Server
 - explained, 270
 - hardware/software requirements, 270
- reports, 19
 - ACS (Audit Collection Services) reports, 522-528
 - Alert Logging Latency report, 513, 515-516
 - Alert reports, 506-508
 - Availability reports, 261-262, 497-498, 508-512
 - Daily Alert report, 513, 519-521
 - delivering, 496-497
 - explained, 260, 493-496
 - exporting, 496
 - Most Common Alerts report, 513, 514-515
 - Performance reports, 498-503
 - Performance Top Objects reports, 504-506
 - running, 261-262
 - Send Queue % Used Top 10 report, 513, 517-519
 - SLT (Service Level Tracking) reports, 532-534
 - SQL Database Space report, 513, 521-522
 - troubleshooting reports that don't show charts, 512-513
- Root Management Server
 - encryption key, 287
 - explained, 265-266
 - hardware/software requirements, 266

rules, 258

security

action and RunAs account security, 282-283

agents, 280

firewalls, 280-281

role-based security model, 278-280

securing DMZ servers with certificates, 283

server and client system monitoring, 17

service-oriented management, 18-19

SLA tracking and reporting, 19

SLDs (Service Level Dashboards)

architecture, 535-537

creating, 539-540

explained, 534-535

installing, 537-539

securing, 540-541

SLT (Service Level Tracking)

explained, 529-530

reports, 532-534

SLOs (Service Level Objectives), 530-531

small enterprise design, 303-305

SNMP device monitoring

explained, 489-490

troubleshooting, 490-491

software requirements, 290-291

synthetic transactions, creating, 621-622

system monitoring, 17-18

Web console

configuring, 765-766

explained, 272

hardware/software requirements, 272

performance view time frame, 377-378

OpsMgrLatencyMonitors container object, configuring, 427-428

Organization State view, 447

OS Capture Account, 84

OS Deployment certificate, 124, 143

OS Deployment Wizard, 206

Out-of-Band Service Point, 75

override management packs, 287, 404-405

overrides, alert tuning with, 405-408

P

P2V (physical-to-virtual) conversions

Convert Physical Server Wizard, 673-679

Additional Properties page, 677

Conversion Information page, 677

Gather System Information page, 674-675

Select Host page, 676

Select Networks page, 677

Select Path page, 676

Select Source page, 674

Summary page, 678-679

Virtual Machine Identity page, 674

Volume Configuration page, 675-676

explained, 45, 672-679

supported operating systems, 672-673

system requirements, 672

Package Status Details report, 898

Package Status Summary report, 898

packages

approving packages to be deployed to device groups, 897-898

checking status of, 898

configuring package programs, 189-190

creating, 189, 206-207, 894, 957-958

defined, 58, 185

OS Deployment certificate, driver management, 208

OS install packages

boot image management, 209

explained, 207-208

task sequence management, 209-210

selecting for approval, 959

uninstalling, 959-960

Password Enabled setting (Exchange Server 2007), 906

Password Expiration setting (Exchange Server 2007), 907

Password History setting (Exchange Server 2007), 907

Password Recovery setting (Exchange Server 2007), 907

passwords

- control configuration options, 41
- resetting, 888-889
- setting password policies for mobile devices, 902-903

patch management, 158-160

patching systems, 10-11, 44, 951-952

Pending Management tree item (OpsMgr), 392-393

performance assessment modeling, 38

performance monitoring, 395-399

Performance Reporting view, 451

Performance reports (OpsMgr), 498-503

Performance Top Objects reports, 504-506

Performance view (Operations Manager console)

- creating, 396-397
- explained, 390

Physical Disk State view, 466

Pilot phase

- OpsMgr deployment, 317-319
- Service Manager deployment, 732-734

PIN control configuration options, 41

Ping Computer Continuously (ping -t) task, 413

Ping Computer task, 413

Ping Computer (with Route) task, 413

PKI (Public Key Infrastructure)

- deploying Enterprise Root CA, 118-120
- explained, 118
- planning, 103
- validating Enterprise Root CA, 120

placement

- of IBCM servers, 106-107
- of VMs (virtual machines)
 - automatic placement, 692-693
 - explained, 692

Placement Settings dialog box, 693-694

Planning reports, 523-524

POC (proof of concept) phase

- OpsMgr deployment, 315-317
- Service Manager deployment, 730-732

policies

- enforcing to mobile devices, 866-867, 902
- group policies, 871-872

- password policies, setting for mobile devices, 902-903

Policy reports, 524

- policy retrieval, 178-181

Policy Refresh Interval setting (Exchange Server 2007), 907

Policy reports, 524

PolicySpy, 67

political management groups, 302

ports (client communication), 82-83

powering on/off virtual guest sessions, 969-970

PowerShell, VMM support for, 633, 640

pre-enrolling devices, 887-888

prefixes

- activity prefixes, 813
- change request prefix, 811-812
- incident prefixes, 761
- problem prefix, 793

Primary Site Server, 68, 114

priority levels

- alerts, 365
- incident priorities, 762-764
- problem priorities, 795-796

Privileged User accounts, configuring, 462-463

Problem Details report, 804

Problem Management Report Library, 800-804

problems (Service Manager)

- analyzing, 797-798
- creating, 796-797
- creating change requests from, 819
- defined, 760, 796
- resolving, 799
- settings
 - explained, 793
 - file attachment limits, 794
 - priority calculation, 795-796
 - problem prefix, 793

Process Monitoring Template, 476-478

processes (Service Manager), 710-711

Production phase

- OpsMgr deployment, 319
- Service Manager deployment, 734

programs, 58, 185

proof of concept (POC) phase

- OpsMgr deployment, 315-317
- Service Manager deployment, 730-732

Protected Distribution Points, 74

protecting data. See DPM (Data Protection Manager) 2010

Protection Agent Installation Wizard, 566-567

protection agents, 565-570

protection groups

- creating, 570-574
- designing, 555-557

provisioning process

- managing, 867-868
- through MDM Self-Service Portal, 886-887

Proxy Management Points, 55-56

PSP (PXE Service Point), 75-76, 94, 115

Public Key Infrastructure. See PKI (Public Key Infrastructure)

Public Receive Queue Size view, 450

Publication State view, 458

Publisher State view, 458

publishing

- announcements, 787-788
- certificate templates, 126-127
- CRL, 119-120
- software, 191-192

PXE Service Point (PSP), 75-76, 94, 115

R

RAID, 99

- RAID 1, 298
- RAID 10, 299
- RAID 5, 298

RAs (review activities), 828

recovering

- Hyper-V host servers, 618-619
- ILR (item-level recovery), 620-619
- SharePoint farms, 609-611

recovering data, DPM (Data Protection Manager) 2010, 580-581

Recovery Wizard, 581, 619

- recovering databases, 592-594
- recovering mailboxes, 594-596

redundancy for OpsMgr

- clustering, 285-286
- explained, 284-285
- management group redundancy, 284

regedit.exe, creating Registry keys with, 223-224

regional server infrastructure

- controlling client access to regional servers, 162-163
- deploying regional site components, 161-162
- explained, 161
- WDS (Windows Deployment Service), 161

registering management groups, 741-743

Registry keys, creating, 223-224

rejecting RAs (review activities), 828

Reload Configuration task, 413

Remote Assist

- accessing systems with, 951
- configuring, 947-950
- explained, 947

remote control, 10, 44

Remote Data Access Service Check monitor, 410

Remote Desktop

- accessing systems with, 933-951
- configuring, 948-949
- explained, 947

Remote Desktop (Admin) task, 414

Remote Desktop (Console) task, 414

Remote Desktop task, 413

Remote Latency view, 451

remote SQL instance, preparing, 560

Remote Tools Client Agent, 97

removing

- CIs (configuration items), 836-838
- VMM (Virtual Machine Manager) user roles, 692

REPADMIN Replsum task, 436

REPADMIN task, 436

Replication Alerts Last 7 Days view, 435

Replication Inbound Bytes/Sec view, 435

Replication Latency view, 435

replication monitoring, 427-431

Replication Performance Overview view, 435
reporting

ACS Reporting, 276-277

Active Directory Management Pack reports,
 437-438

AI (Asset Intelligence)

report categories, 247

reporting classes, 236-241

change management reports

Activity Management Report Library, 841

Change Management Report Library,
 840-841

Configuration Management Report
 Library, 842-843

explained, 838-839

Service Manager report controls, 839

with Configuration Manager

explained, 64, 228-231

legacy reports, 231

Reporting Services reports, 231-234

software metering reports, 234-235

consolidated reporting, 34

with Cross Platform Management Packs,
 467-468

custom reports, 231

DCM Compliance reports, 246-253

with Exchange 2007 Management Pack,
 453-454

incident and problem reports

explained, 799

Incident Management Report Library,
 800-804

Problem Management Report Library,
 800-804

Service Manager report controls,
 799-800

with MDM (Mobile Device Manager)

Device Status Details, 898

Device Status Summary, 898

Package Status Details, 898

Package Status Summary, 898

with OpsMgr

ACS (Audit Collection Services) reports,
 522-528

Alert Logging Latency report, 513,
 515-516

Alert reports, 506-508

Availability reports, 261-262, 497-498,
 508-512

Daily Alert report, 513, 519-521

delivering reports, 496-497

explained, 19, 260, 493-496

exporting reports, 496

Most Common Alerts report, 513,
 514-515

Performance reports, 498-503

Performance Top Objects reports,
 504-506

running reports, 261-262

Send Queue % Used Top 10 report,
 513, 517-519

SLT (Service Level Tracking) reports,
 532-534

SQL Database Space report, 513,
 521-522

troubleshooting reports that don't show
 charts, 512-513

with SCCM (System Center Configuration
 Manager), 12

with SCCP (System Center Capacity
 Planner), 39

SLA tracking and reporting, 19

with SQL Server Management Pack,
 460-461

with System Center Essentials, 45,
 972-973

with VMM (Virtual Machine Manager), 669

with Windows Management Pack, 421-423

Reporting data warehouse

explained, 269-270

hardware/software requirements, 270

reporting database, 296

Reporting option (SCE), 934-935

Reporting Point (RP), 77, 115

Reporting Server

- explained, 270

- hardware/software requirements, 270

Reporting Service Point (RSP), 77, 115**Reporting Services reports**

- creating, 231-232

- scheduling, 232-234

ReportingServicesService.exe.config file, 512-513**requesting**

- certificates for mutual authentication, 355-356

- Document Signing Certificate, 140-143

- OS Deployment certificate, 143

- root CA certificates, 353-355

Require Device Encryption setting (Exchange Server 2007), 907**Require encrypted S/MIME messages setting (Exchange Server 2007), 908****Require Manual Synchronization While Roaming setting (Exchange Server 2007), 908****Require Storage Card Encryption setting (Exchange Server 2007), 908****resetting passwords, 888-889****Resident Management Point, 174****resolution times, 764-765****resolving**

- critical events, 942-944

- incidents, 791-793

- problems, 799

response time alerts, configuring, 963-964**Restart Health Service Recovery, 363-364****restoring**

- Exchange databases, 592-594

- mailboxes, 594-596

- SQL Server databases, 600-602

resuming change requests, 826-827**returning to activities, 827-828****review activities (RAs), 828****Review Activity Details report, 841****reviewers, adding to change requests, 824-825****reviewing Central Site status, 146****RFC Details report, 840****RMS. See Root Management Server****roaming (client), 56-57****role-based access control, 635-637****role-based security model, 278-280****roles, server. See servers****root CA certificates**

- installing on SCE server, 974-975

- requesting, 353-355

Root Management Server

- encryption key, 287, 380-381

- explained, 265-266

- hardware/software requirements, 266

RoutePrint task, 420**RP (Reporting Point), 77, 115, 151-152****Rsetup.log files, 151-152****RSP (Reporting Service Point), 77, 115, 152-153****rules**

- explained, 258

- Memory Pool Non-Paged Bytes, 416

- Memory Pool Paged Bytes, 416

- performance collection rules, 395-396

- SQL Server Service Broker Manager Has Shutdown, 456

- Total Processor % Interrupt Time, 416

Run Chkdsk, 420**Run Chkntfs, 420****Run Home Page Summarization action, 195****RunAs accounts, 283****S****sample distributed applications, 488-489****SAN (storage area network), 297-299, 717**

- SAN transfers, 639

- when to use, 98-100

Sanbolic Clustered File System (CFS), 639-640**saving**

- incident and problem reports, 803

- virtual guest sessions, 970

SCCM (System Center Configuration Manager) 2007. See ConfigMgr

SCCP (System Center Capacity Planner)

- business solutions addressed by, 37-38
- capacity models, 38-39
 - basic infrastructure requirements, 851
 - capabilities, 850
 - creating with Model Wizard, 853-860
 - editing with Model Editor, 860-862
 - simulations, 862-863
- current usage analysis, 39
- explained, 8, 37, 844-846
- Hardware Editor
 - adding/modifying computers, 852
 - adding/modifying devices, 852
 - explained, 847, 851-852
 - list icons, 852
- hardware requirements, 848-849
- history and revisions, 39
- installing, 849-850
- main screen, 37
- Model Editor, 847, 860-862
- Model Wizard
 - Application page, 858-859
 - Client-Only Sites page, 854-855
 - explained, 847, 853
 - Hardware page, 857-858
 - Mailbox Sites page, 853-854
 - Model Summary page, 859-860
 - Networks page, 855-856
 - starting, 853
- performance assessment modeling, 38
- reporting, 39
- SCCP 2006, 847
- SCCP 2006 SP1, 848
- SCCP 2007, 848
- Simulation, 847
- software requirements, 849
- supported operating systems, 849
- SCE (System Center Essentials) 2010. See System Center Essentials**
- SCE Configuration Wizard, 924-928**
- SCE Reporting Services, installing, 929-930**
- Schedule Home Page Summarization action, 195**

scheduling

- Alert Logging Latency report, 515-516
- Availability reports, 510-512
- client schedules, 104-105
- Daily Alert report, 519-521
- Most Common Alerts report, 514-515
- Performance reports, 499-503
- Performance Top Objects reports, 505-506
- Reporting Services reports, 232-234
- Send Queue % Used Top 10 report, 517-519
- SQL Database Space report, 521-522

SCOM (System Center Operations Manager) 2007. See OpsMgr**scope**

- defining for VMM (Virtual Machine Manager), 644-645
- of DPM (Data Protection Manager) projects, 554

scripts

- AddNewClusteredVM.ps1, 617-618
- AddNewStandAloneVM.ps1, 617-618

SCSM (System Center Service Manager) 2010. See Service Manager**SDK and Configuration service account, 282****sealing management packs via command line, 486****searching CIs (configuration items), 836-837****Secondary Sites, 55-56, 114****SecureStorageBackup tool, 754****security**

- ConfigMgr
 - management console, 80-82
 - Mixed mode security, 79-80
 - Native mode security, 79-80, 102-104
 - port requirements, 82-83
 - server communication, 80
 - service account security, 83-84
- OpsMgr security
 - action and RunAs account security, 282-283
 - agents, 280

- firewalls, 280-281
- role-based security model, 278-280
- SLDs (Service Level Dashboards), 540-541
- security-based management groups, 302**
- Select Backup Destination dialog box, 754**
- Select Host page**
 - Convert Virtual Server Wizard, 681-682
 - Deploy Virtual Machine Wizard, 695
- Select Networks page**
 - Convert Virtual Server Wizard, 682
 - Deploy Virtual Machine Wizard, 696
- Select Path page**
 - Convert Physical Server Wizard, 676
 - Convert Virtual Server Wizard, 682
 - Deploy Virtual Machine Wizard, 696
- Select Source page (Convert Physical Server Wizard), 674, 676**
- Select Virtual Machine Source dialog box, 681-680**
- self-service access (SCSM), 34-35**
- self-service management (MDM), 41-42**
- Self-Service Portal**
 - creating change requests from, 819-821
 - creating incidents with, 779-781
 - creating VMs with, 703-699
 - designing, 648
 - device provisioning through, 886-887
 - explained, 632
 - hardware requirements, 643
 - installing, 656-657, 884-885
 - software requirements, 643-644
 - supported operating systems, 643
- Self-Service User role (VMM), 684, 686-687**
- Send Queue % Used Top 10 report, 513, 517-519**
- Server Authentication certificate templates, 124-126**
- Server Certificate, 103, 115**
- Server Locator Point (SLP), 77-78, 114**
- Server Management Suite Datacenter (SMSD) licenses, 47**
- Server Management Suite Enterprise (SMSE) licenses, 47**
- Server Management Suite licenses, 47**

Server State view, 447, 466**servers**

- Active Directory and group policies, 871-872
- CAS Server role, monitor and rule sync times, 441
- Central Site Server, 68, 114, 143-145
- checking health of, 945
- Component Servers, 114
- converting to virtual guest sessions, 967-968
- Device Management server, 870-871
- DMZ servers, monitoring with certificates, 283
 - configuring agents to use certificates, 358
 - creating certificate templates, 353
 - explained, 352-353
 - installing agents on DMZ servers, 356-357
 - requesting certificates from root CA for mutual authentication, 355-356
 - requesting root CA certificates, 353-355
- DPM (Data Protection Manager) server
 - designing, 558-559
 - preparation, 559-560
- Enrollment server, 871
- Exchange Server
 - and MDM (Mobile Device Manager), 904-908
 - protecting with DPM (Data Protection Manager), 588-598
- explained, 870
- file servers, protecting with DPM (Data Protection Manager), 584-586
- Gateway server, 871
 - explained, 273-274
 - hardware/software requirements, 274
- Hyper-V host servers
 - adding, 965
 - automatically protecting new machines, 617-618
 - creating host groups, 666-667
 - host clusters, 667-668
 - managing, 667-668

- protecting, 615-617
- recovering, 618-619
- VMM (Virtual Machine Manager). *See*
VMM (Virtual Machine Manager)
- installing for MDM (Mobile Device
Manager), 880-884
- management console, 870
- Management Server
 - explained, 266-268
 - hardware/software requirements,
267-268
- MDM SQL Server, 871
- monitoring with SCOM (System Center
Operations Manager), 17
- preparing for MDM (Mobile Device
Manager), 877
- prerequisites, 875-876
- Primary Site Server, 68, 114
- putting into Maintenance mode, 945-947
- regional server infrastructure
 - controlling client access to regional
servers, 162-163
 - deploying regional site components,
161-162
 - explained, 161
 - WDS (Windows Deployment Service),
161
- Reporting Server
 - explained, 270
 - hardware/software requirements, 270
- Root Management Server
 - encryption key, 287
 - explained, 265-266
 - hardware/software requirements, 266
- Secondary Site Servers, 114
- securing server communication, 80
- Site Database, 114
- Site System, 114
- SLP (Server Locator Point), 114
- SMS Provider, 114
- SQL Server
 - EUR Client, 603-604
 - installing, 130-132
 - local firewall configuration, 132-133

- protecting with DPM (Data Protection
Manager), 598-605
- SQL service accounts, creating, 129
- VMM Server
 - deployment, 649-654
 - designing, 647-648
 - explained, 631-633
 - hardware requirements, 640
 - installing, 651-654
 - remote SQL instance requirements, 641
 - software requirements, 641
 - supported operating systems, 641
- Service Level Dashboards. *See* SLDs (Service
Level Dashboards)**
- Service Level Dashboards Solution
Accelerator, 260**
- Service Level Objectives (SLOs), 530-531**
- Service Level Tracking. *See* SLT (Service Level
Tracking)**
- Service Manager**
 - architecture, 711-713
 - backing up
 - backup schedules, 753-754
 - encryption key, 756
 - ServiceManager database, 754-756
 - business solutions addressed by, 33-34
 - change management. *See* change
management
 - console, 33
 - consolidated reporting, 34
 - deployment
 - Active Directory connector, 747-748
 - components, 735-738
 - Configuration Manager connectors,
752-753
 - data warehouse, 738-741
 - Extract, Transform, and Load (ETL) jobs,
743-744
 - management group registration,
741-743
 - Operations Manager connector, 748-752
 - steps, 735
 - Web Portals, 744-746

- design scenarios, 719
 - large enterprise design, 724-726
 - medium enterprise design, 722-724
 - small enterprise design, 720-722
- disk performance, 717
- explained, 8, 33, 707-710
- hardware requirements, 714-715
- history and revisions, 35-36
- incident management. *See* incident management
- phases of project deployment
 - Design and Planning phase, 728-730
 - Design Principles Training phase, 728
 - Pilot phase, 732-734
 - POC (proof of concept) phase, 730-732
 - Production phase, 734
 - time estimates per phase, 734-735
- processes, 710-711
- project phases, 726-727
- SAN versus DAS, 717
- self-service access, 34-35
- software requirements, 716-717
- SQL versions, choosing, 717-719
- technologies, 711
- service-level agreement, 19**
- service-oriented management, 18-19**
- Set Database Offline task, 459**
- Set Database Online task, 459**
- Set Database to Emergency State task, 459**
- Set-EnrollmentConfig command, 884**
- SETSPN task, 436**
- SFW (Veritas Storage Foundation 5.1 for Windows), 640**
- SharePoint farms**
 - content database recovery, recovering, 611
 - data sources and recoverable data, 605
 - item-level recovery, 611
 - preparing for protection, 606-607
 - protecting with DPM (Data Protection Manager), 607-609
 - recovering, 609-611
- Show Failed Rules and Monitors for This Health Service task, 414**
- Show Running Rules and Monitors for This Health Service task, 414**
- Simulation (Capacity Planner), 847**
- simulations of capacity models, 862-863**
- single-server OpsMgr 2007 R2 install, 324-329**
- single-server VMM deployment, 650**
- Site Databases, 114**
- Site Server databases, 69-70**
- Site Service State view, 447**
- Site System, 114, 149-150**
- Site System Status page (ConfigMgr), 146**
- site topology (AD), 116-117**
- Site Topology view (Model Editor), 860-861**
- sites (SharePoint), recovering, 611**
- site-specific configuration settings, 92-93**
- sizing databases, 89-90, 292-294**
- SLA (service-level agreement), tracking and reporting, 19**
- SLDs (Service Level Dashboards)**
 - architecture, 535-537
 - creating, 539-540
 - explained, 534-535
 - installing, 537-539
 - securing, 540-541
- SLOs (Service Level Objectives), 530-531**
- SLP (Server Locator Point)**
 - deployment, 150-151
 - explained, 77-78, 114
- SLT (Service Level Tracking)**
 - explained, 529-530
 - reports, 532-534
 - SLOs (Service Level Objectives), 530-531
- small enterprise design**
 - ConfigMgr, 107
 - OpsMgr, 303-305
 - Service Manager, 720-722
- SMP (State Migration Point)**
 - explained, 76, 115
 - placement of, 94
- SMS (Systems Management Server)**
 - SMS 2003 (SMS v3.0), 13
 - SMS Provider, 68-69, 114
 - SMS v1.x, 12-13
 - SMS v2.0, 13
- sms_def.mof file, editing, 226**

SMSD (Server Management Suite Datacenter)
 licenses, 47

SMSE (Server Management Suite Enterprise)
 licenses, 47

SMSFSPSetup.log file, 151

SMSReportingInstall.log file, 151-152

SMTP notification channel, configuring, 771-772

snapshots of virtual guest sessions, managing, 971-972

SNK (Strong Name Key) files, 486

SNMP
 device monitoring, 489-490
 troubleshooting, 490-491

Software 01A-12A reporting classes, 239-241

software distribution
 configuring package programs, 189-190
 configuring software sources, 185
 creating software packages, 189, 894
 customizing installation, 187-188
 deploying software automatically, 193-194
 explained, 11, 44, 58, 185-186
 monitoring software deployment, 195
 publishing software, 191-192
 selecting Distribution Points, 190-191
 update distribution
 deploying software updates, 200-201
 deployment templates, 196-197
 explained, 196
 managing update deployment, 201-202
 monitoring software update deployment, 202-203
 Software Updates Client Agent, 196-197
 update lists, 198-199

software inventory, 61-62

Software Inventory Client Agent, 97

software licensing data, importing, 243-245

software metering
 explained, 61-63, 234
 reports, 234-235
 Software Metering Client Agent, 234

Software Metering Client Agent, 97, 234

Software option (SCE), 933-934

software packages. *See* **packages**

software reports (AI), 247

software requirements
 ConfigMgr, 87-88
 for DPM (Data Protection Manager), 552-553
 for OpsMgr, 290-291
 ACS (Audit Collection Services), 277
 audit collection database, 276
 audit collector, 275
 Connector Framework, 278
 Gateway server, 274
 management server, 268
 Operations Console, 271
 Operations Manager database, 268-269
 Reporting data warehouse, 270
 Reporting Server, 270
 Root Management Server, 266
 Web console, 272
 for SCCP (System Center Capacity Planner), 849
 for Service Manager, 716-717
 for VMM (Virtual Machine Manager)
 Administrator Console, 642
 Self-Service Portal, 643-644
 VMM Server, 641

software sources, configuring, 185

Software Update Client Agent, 97

Software Update Point (SUP), 78, 115, 158-160

Software Updates - A Compliance folder, 202

Software Updates Client Agent, 196-197, 222

Software Updates home page, 196

SPN Health task, 436

SQL Database Space report, 513, 521-522

SQL Management Studio task, 459

SQL Profiler task, 459

SQL Server
 choosing version of
 ConfigMgr, 100-101
 Service Manager, 717-719
 databases
 protecting, 598-600
 restoring, 600-602
 SQL End User Recovery, 602-605

Enterprise Edition, 100, 299-301
 EUR Client, 603-604
 explained, 871
 installing, 130-132
 licensing costs, 99-101
 local firewall configuration, 132-133
 prerequisites, 875-876
 remote SQL instance

preparing, 560

VMM Server requirements, 641

SQL Server Management Pack

configuring, 455

explained, 454-455

reports, 460-461

tasks, 459-460

tuning, 455-457

views, 457-459

SQL service accounts, creating, 129

Standard Edition, 100, 299-301

System Center Essentials support for, 918

SQL Server Management Pack

configuring, 455

explained, 454-455

reports, 460-461

tasks, 459-460

tuning, 455-457

views, 457-459

SQL Server Service Broker Manager Has Shutdown rule, 456

SSL

Certificate Services website for SSL, 128-129

configuring, 136-137

Standard (SMB) Distribution Points, 73

Standard Edition (SQL Server), 100

Start Audit Collection task, 414

Start Online Store Maintenance task, 414

Start WMI Service task, 414

starting Model Wizard, 853

State Migration Point (SMP), 76, 94, 115

State view (Operations Manager console), 389

status of packages, checking with MDM (Mobile Device Manager), 898

storage area network (SAN), 98-100, 297-299, 717

storage pool, adding disks to, 563-564

storage requirements, calculating, 557-558

Strong Name Key (SNK) files, 486

Subscription State view, 458

subscriptions, configuring, 364-367

Summary page

Convert Physical Server Wizard, 678-679

Convert Virtual Server Wizard, 682-683

Deploy Virtual Machine Wizard, 697

SUP (Software Update Point), 78, 115, 158-160

SUPSetup.log file, 159

SvcMgr. See Service Manager

synchronization

AI (Asset Intelligence) catalog, 235-236

CAS role monitor and rule sync times, 441

mailbox monitor and rule sync times, 442

SUP (Software Update Point), 159-160

synthetic transactions, creating, 621-622

System Center Configuration Manager (SCCM) 2007. See ConfigMgr

System Center Data Protection Manager. See DPM (Data Protection Manager) 2010

System Center Essentials

administration

monthly tasks, 983-984

regular tasks, 981

weekly tasks, 982-983

agents

installing on domain-attached systems, 973-974

installing on nondomain joined systems, 974-977

asset tracking, 44

business solutions addressed by, 43-44, 912

computer and device discovery

autodiscover, 938-939

explained, 937-938

manually discovering computers, 939-940

manually discovering network devices, 940-941

- console, 43
- explained, 8, 43, 910-911
- history and revisions, 45-46
 - System Center Essentials 2007, 913-914
 - System Center Essentials 2007 SP1, 914-915
 - System Center Essentials 2010, 915-916
- installing on separate servers
 - management console tools, 928-929
 - SCE Reporting Services, 929-930
- installing on single server
 - preparation, 920
 - running SCE Configuration Wizard, 924-928
 - running SCE installation, 921-923
- inventory
 - collecting manually, 960-961
 - explained, 960
 - viewing, 960
- management console
 - Administration option, 935-937
 - Authoring option, 937
 - Computers option, 931
 - explained, 930-931
 - installing management console tools, 928-929
 - Monitoring option, 932-933
 - Reporting option, 934-935
 - Software option, 934
 - Updates option, 933-934
- monitoring
 - alerts, 942
 - checking health of servers, 945
 - explained, 941-942
 - handling warning events, 944-945
 - putting servers in Maintenance mode, 945-947
 - resolving critical events, 942-944
- monitoring and alerting, 44
- P2V (physical-to-virtual) conversions, 45
- packages
 - creating, 957-958
 - selecting for approval, 959
 - uninstalling, 959-960
- patching/updating systems, 44, 951-952
- prerequisites
 - hardware requirements for multiserver configuration, 918
 - hardware requirements for single-server configuration, 918
 - multisite configuration, 919
 - supported and unsupported scenarios, 919-920
 - supported operating systems, 917-918
 - supported versions of SQL Server, 918
- Remote Assist
 - accessing systems with, 951
 - configuring, 947-950
 - explained, 947
- Remote Desktop
 - accessing systems with, 933-951
 - configuring, 948-949
 - explained, 947
- remote support, 44
- reporting, 45, 972-973
- root CA certificates, installing, 974-975
- software distribution, 44
- technical solutions addressed by, 912-913
- troubleshooting
 - email host server addresses, 979
 - Firewall Rule exceptions, 978-979
 - Not Connected errors, 979-980
 - virtual network switches, 980
- updates
 - approving/declining, 954-956
 - explained, 951-952
 - setting deadlines on, 956-957
 - uninstalling, 956
 - update management settings, 952-954
 - viewing, 954
- virtual host management, 44-45
- virtualization management
 - accessing virtual guest sessions, 970

- changing “hardware” of virtual guest sessions, 970-971
- converting physical servers to virtual guest sessions, 967-968
- creating virtual guest sessions, 965-967
- designating Hyper-V host servers, 965
- importing VMware guest sessions to Hyper-V, 968-969
- managing snapshots of guest sessions, 971-972
- powering on/off virtual guest sessions, 969-970
- saving virtual guest sessions, 970
- website monitoring agents
 - creating, 961-963
 - response time alerts, 963-964

System Center Mobile Device Manager. See MDM (Mobile Device Manager)

System Center Online Services, 246-247

System Center Operations Manager. See OpsMgr

System Center Service Manager. See Service Manager

System Center Virtual Machine Manager. See VMM (Virtual Machine Manager)

System Integrity reports, 524

system inventory. See inventory

System Management container, creating with ADSI Edit, 134-135

system monitoring. See monitoring

System State

- backing up, 587
- protecting with DPM (Data Protection Manager), 586-587

systems management in the enterprise, 6-7

Systems Management Server. See SMS (Systems Management Server)

T

tape libraries, configuring, 564-565

tape-based backup technologies, 545-546

task sequences, creating, 209-210

Task Status view, 390, 457

tasks

- in Active Directory Management Pack, 436-437
- in Exchange 2007 Management Pack, 452-453
- in Operations Manager Management Pack, 412-414
- in SQL Server Management Pack, 459-460
- in Windows Management Pack, 418-421

TCP Port Template, 477-479

templates

- certificate templates
 - creating, 353
 - explained, 103-104
- change request templates, 814-815
- Client Authentication certificate template, 122-123
- deployment templates, 59, 196-197
- Document Signing Certificate template, 126
- Group Policy templates, installing, 898-900
- Management Pack Templates
 - explained, 468-469
 - OLE DB Data Source Template, 474-476
 - Process Monitoring Template, 476-478
 - TCP Port Template, 477-479
 - Unix/Linux Log File Template, 478-479
 - Unix/Linux Service Template, 480
 - Web Application Template, 469-471
 - Windows Service Template, 471-474
- notification templates, 772-773
- publishing certificate templates, 126-127
- report templates, 972-973

time estimates for OpsMgr project deployment, 320

Total Processor % Interrupt Time rule, 416

Trace32.exe, 146, 149

tracking

- assets, 10, 44
- CAL license tracking, 241-242
- devices, 41
- mobile devices, 867
- SLA tracking and reporting, 19
- SLT (Service Level Tracking), 529-530

Transaction Log Free Space view, 457-458**transactions**

- intraorganization synthetic transactions, configuring, 443-444
- synthetic transactions, creating, 621-622

Transport DSN view, 449**Transport Queues view, 449****troubleshooting. *See also* incident management**

- operating system deployment, 212-213
- reports that don't show charts, 512-513
- Service Manager troubleshooting tasks, 788-791
- SNMP device monitoring, 490-491
- System Center Essentials
 - email host server addresses, 979
 - Firewall Rule exceptions, 978-979
 - Not Connected errors, 979-980
 - virtual network switches, 980

tuning

- SQL Server Management Pack, 455-457
- Windows Management Pack, 416-415

U

UM Connectivity Call Latency view, 451**Unapproved InROM application list setting (Exchange Server 2007), 908****Unified Messaging Server Alerts view, 451****Unified Messaging Server State view, 451****uninstalling**

- packages, 959-960
- updates, 956

UNIX Action Account profile, assigning Linux Non-Privileged Users to, 464**UNIX agents, installing, 349-352****UNIX Privileged Account profile, assigning Linux Privileged Users to, 464-465****Unix/Linux Log File Template, 478-479****Unix/Linux Service Template, 480****unknown computer support, 210-212****Update Repository container, 59****updates**

- approving/declining, 954-956
- for devices, 41
- for management packs, 371-372
- software update distribution, 59
- for systems, 10-11
- update distribution
 - deploying software updates, 200-201
 - deployment templates, 196-197
 - explained, 196
 - managing update deployment, 201-202
 - monitoring software update deployment, 202-203
 - Software Updates Client Agent, 196-197
 - update lists, 198-199
- update lists, 59, 198-199
- via System Center Essentials
 - explained, 951-952
 - setting deadlines on updates, 956-957
 - uninstalling updates, 956
 - update management settings, 952-954
 - viewing updates, 954

Updates option (SCE), 933-934**updating systems, 44****Usage reports, 524****User Connection view, 458****User Role Properties dialog box, 685, 691****User State Migration Tool (USMT) package, creating, 207****users**

- adding to groups, 541
- discovery, 91-92
- user roles (VMM)
 - Administrator, 684-686
 - Delegated Administrator, 684, 686-687
 - modifying roles, 690-691
 - removing roles, 692
 - Self-Service User, 684, 686-687

USMT (User State Migration Tool) package, creating, 207

V

V2V conversions, 679-683

validating

- Central Site installation, 145-147
- Enterprise Root CA, 120
- inventory data, 227

Veritas Storage Foundation 5.1 for Windows (SFW), 640

viewing

- inventory, 228, 960
- updates, 954

views

- in Active Directory Management Pack, 432-436
- in Cross Platform Management Packs, 465-466
- in Exchange 2007 Management Pack, 447-452
- in Model Editor, 860-861
- in Operations Manager Management Pack, 410-412
- in SQL Server Management Pack, 457-459
- in Windows Management Pack, 416-419

virtual guest sessions

- accessing, 970
- changing “hardware” of, 970-971
- converting physical servers to, 967-968
- creating, 965-967
- importing VMware guest sessions to Hyper-V, 968-969
- managing snapshots of, 971-972
- powering on/off, 969-970
- saving, 970

virtual host management, 44-45

virtual machine hosts, 644

Virtual Machine Identity page

- Convert Physical Server Wizard, 674
- Convert Virtual Server Wizard, 680-681

Virtual Machine Manager. *See* VMM (Virtual Machine Manager)

virtual network switches, 980

virtualization management

with System Center Essentials

- accessing virtual guest sessions, 970
- changing “hardware” of virtual guest sessions, 970-971
- converting physical servers to virtual guest sessions, 967-968
- creating virtual guest sessions, 965-967
- designating Hyper-V host servers, 965
- importing VMware guest sessions to Hyper-V, 968-969
- managing snapshots of guest sessions, 971-972
- powering on/off virtual guest sessions, 969-970
- saving virtual guest sessions, 970
- virtual network switches, 980

virtualized environments, protecting with DPM (Data Protection Manager)

- automatically protecting new machines, 617-618
- explained, 615
- ILR (item-level recovery), 620-619
- protecting Hyper-V virtual machines, 615-617
- recovering Hyper-V virtual machines, 618-619

with VMM (Virtual Machine Manager). *See* VMM (Virtual Machine Manager)

VMM (Virtual Machine Manager)

- Administrator Console
 - explained, 631, 666-667
 - hardware requirements, 642
 - installing, 654-656
 - software requirements, 642
 - supported operating systems, 642

Agent

- explained, 632
- installing, 657-661
- business solutions addressed by, 29-30, 628-629
- capabilities, 30-31
- cluster support, 634-635

- command shell, 670-671
- console, 29
- deployment
 - Administrator Console, 654-656
 - Agent, 657-661
 - database considerations, 650
 - multiple-server deployment, 650
 - Self-Service Portal, 656-657
 - single-server deployment, 650
 - VMM Server, 649-654
- environment, 644-645
- explained, 7-8, 28-29, 626-628, 631, 663-665
- heterogeneous management, 634
- history and revisions, 31-32
 - early virtualization management techniques, 637
 - VMM 2007, 637
 - VMM 2008, 637-638
 - VMM 2008 R2, 638-640
- hosts
 - creating host groups, 666-667
 - host clusters, 667-668
 - managing, 667-668
- library
 - configuring, 668-669
 - designing, 643-649
 - explained, 632-633
- Maintenance mode, 639
- managing, 670
- monitoring capabilities, 669
- P2V (physical-to-virtual) conversions
 - Convert Physical Server Wizard, 673-679
 - explained, 672-679
 - supported operating systems, 672-673
 - system requirements, 672
- planning for deployment
 - defining project scope, 645-646
 - designing database server and database, 648
 - designing library servers and libraries, 643-649

- designing Self-Service Portal, 648
- designing VMM Server, 647-648
- determining number of VMM instances, 646-647
- determining Operation Manager integration, 646
- understanding environment, 644-645
- PowerShell support, 633
- reporting, 669
- role-based access control, 635-637
- Self-Service Portal
 - designing, 648
 - explained, 632
 - hardware requirements, 643
 - installing, 656-657
 - software requirements, 643-644
 - supported operating systems, 643
- technical solutions addressed by, 629-630
- user roles
 - Administrator, 684-686
 - Delegated Administrator, 684, 686-687
 - modifying, 690-691
 - removing, 692
 - Self-Service User, 684, 687-690
- V2V conversions, 679-683
- VMM Server
 - designing, 647-648
 - explained, 631-633
 - hardware requirements, 640-641
 - installing, 651-654
 - preparing for deployment, 649-650
 - remote SQL instance requirements, 641
 - software requirements, 641
 - supported operating systems, 641
- VMs (virtual machines)
 - automatic placement, 692-693
 - creating with Self-Service Portal, 697-699
 - customizing host ratings for, 693-695
 - deploying with Administrator Console, 695-697
 - managing, 669

- migrating, 699-705
- system requirements, 644

VMs (virtual machines)

- creating with Self-Service Portal, 697-699
- customizing host ratings for, 693-695
- deploying with Administrator Console, 695-697
- managing, 669
- migrating, 699-705
 - dragging and dropping VM onto host group, 705
 - dragging and dropping VM onto host server, 704
- Migrate Storage action, 702-703
- Migrate Virtual Machine Wizard, 701-702
- supported storage migration technologies, 701
- supported virtual machine migration technologies, 700-706

- P2V (physical-to-virtual) conversions, 672-679

- Convert Physical Server Wizard, 673-679
 - explained, 672
 - supported operating systems, 672-673
 - system requirements, 672

- placement

- automatic placement, 692-693
 - explained, 692

- V2V conversions, 679-683

- VMware guest sessions, importing to Hyper-V, 968-969

- Volume Configuration page (Convert Physical Server Wizard), 675-676

- Volume Information task, 420

W

- Wake On LAN (WOL), 71

- warning alerts, 365

- warning events, 944-945

- Watcher nodes, 962-963

- WDS (Windows Deployment Service), 161

- Web Application Template, 469-471

- Web console

- explained, 259, 272, 390-391
 - hardware/software requirements, 272
 - performance view time frame, 377-378

- Web Page view (Operations Manager console), 390

- Web Portals, installing, 744-746

- WebDAV, configuring, 137-138

- website monitoring agents

- creating, 961-963
 - response time alerts, 963-964

- weekly administration tasks (SCE), 982-983

- Win32Reg_CompanyABC_Warranty class, validating, 227

- Windows 7, Remote Assist configuration, 948

- Windows Computers tasks, 418-421

- Windows Deployment Service (WDS), 161

- Windows Management Pack

- configuring, 415
 - explained, 415
 - reports, 421-423
 - tasks, 418-421
 - tuning, 416
 - views, 416-419

- Windows Preinstallation Environment, 60

- Windows Server 2003, Remote Desktop configuration, 948

- Windows Server 2008 R2, Remote Desktop configuration, 949

- Windows Server 2008, Remote Desktop configuration, 948

- Windows Server Update Services (WSUS)

- configuring WSUS website for SSL, 139-140
 - installing, 138-139

- Windows Service Template, 471-474

- Windows Vista, Remote Assist configuration, 948

- Windows XP, Remote Assist configuration, 947-948

- WinPE, 60, 203

- wiping devices, 890-892

wizards

Add Hosts Wizard, 657-659

Capacity Planner Model Wizard, 847

Convert Physical Server Wizard, 673-679

- Additional Properties page, 677
- Conversion Information page, 677
- Gather System Information page, 674-675
- Select Networks page, 677
- Select Path page, 676, 682
- Select Source page, 674, 676
- Summary page, 678-679, 682-683
- Virtual Machine Identity page, 674
- Volume Configuration page, 675-676

Convert Virtual Server Wizard, 679-683

- Additional Properties page, 682
- Select Host page, 681-682
- Select Networks page, 682
- Virtual Machine Identity page, 680-681

Create New Protection Group Wizard, 570-574, 589-592, 616-617

Create User Role Wizard, 687-690

Deploy Virtual Machine Wizard, 695-697

DPM Setup Wizard, 561-562

Migrate Virtual Machine Wizard, 701-702

Model Wizard

- Application page, 858-859
- Client-Only Sites page, 854-855
- explained, 853
- Hardware page, 857-858
- Mailbox Sites page, 853-854
- Model Summary page, 859-860
- Networks page, 855-856
- starting, 853

New Package Wizard, 189

New Site Role wizard, 158-159

Office Customization Wizard, 187-188

OS Deployment Wizard, 206

Protection Agent Installation Wizard, 566-567

Recovery Wizard, 619

- recovering databases, 592-594

- recovering mailboxes, 594-596

Recovery Wizard (DPM), 581

SCE Configuration Wizard, 924-928

WSUS Configuration Wizard, 139

WOL (Wake On LAN), 71

workflow engine (Service Manager), 711

workflows (change request), 815-816

WSUS (Windows Server Update Services)

- configuring WSUS website for SSL, 139-140

- installing, 138-139

WSUS Configuration Wizard, 139

WSUSCtrl.log file, 159

WSUSUtil.exe, 140