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 administers 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

IN THIS CHAPTER

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

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.

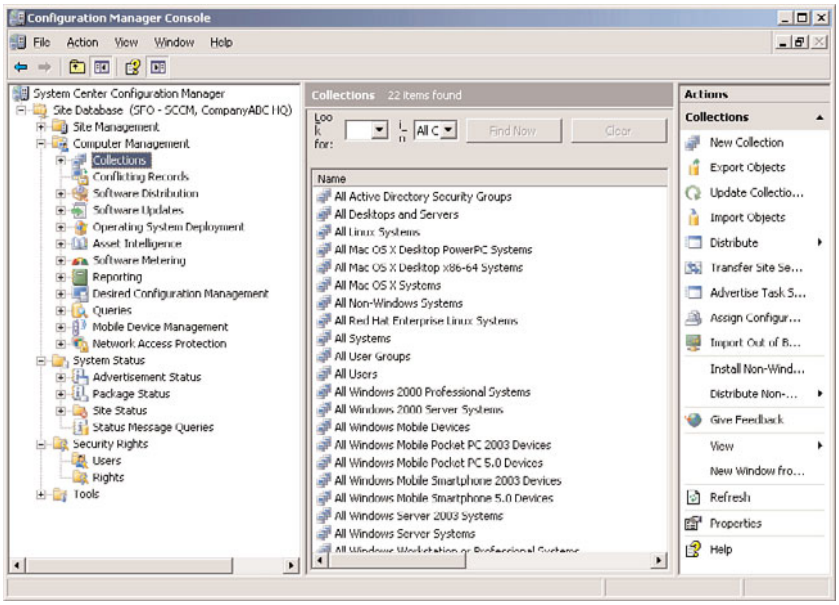

FIGURE 1.1 The System Center Configuration Manager console.

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.

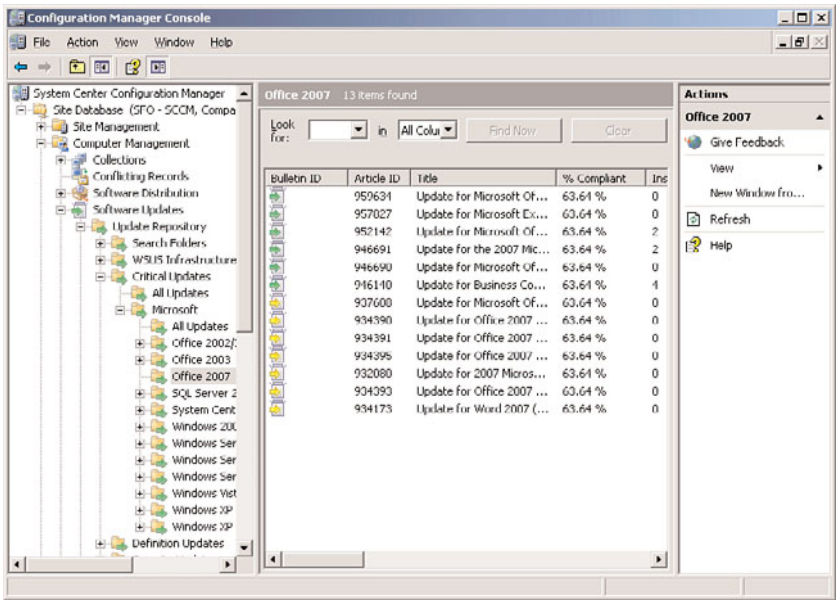

FIGURE 1.2 Details in the SCCM console relative to patching and updating systems.

- **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.

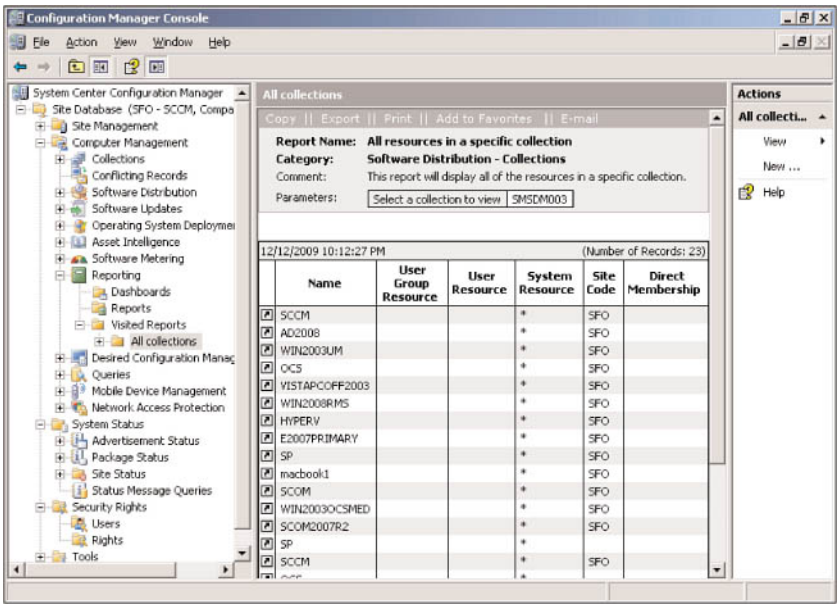

FIGURE 1.3 Reports tool built in to SCCM.

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.

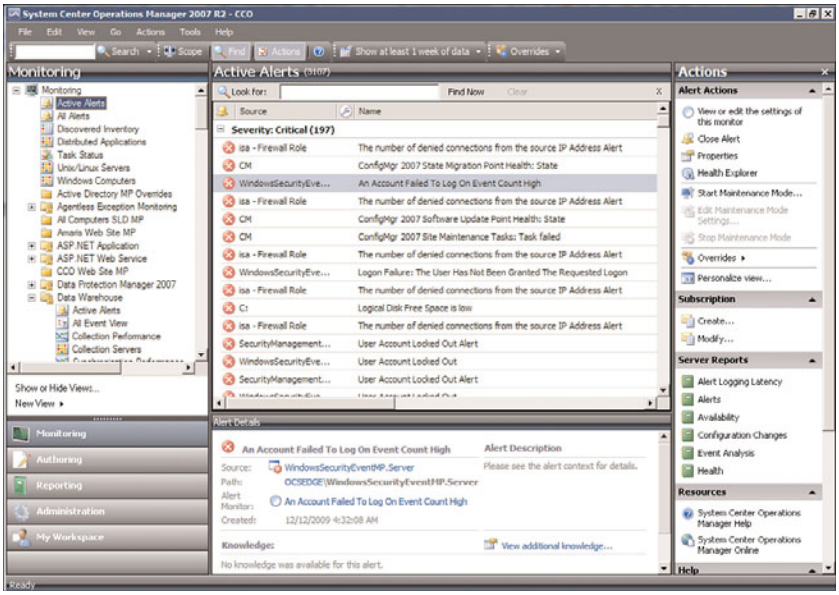

FIGURE 1.4 The System Center Operations Manager console.

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.

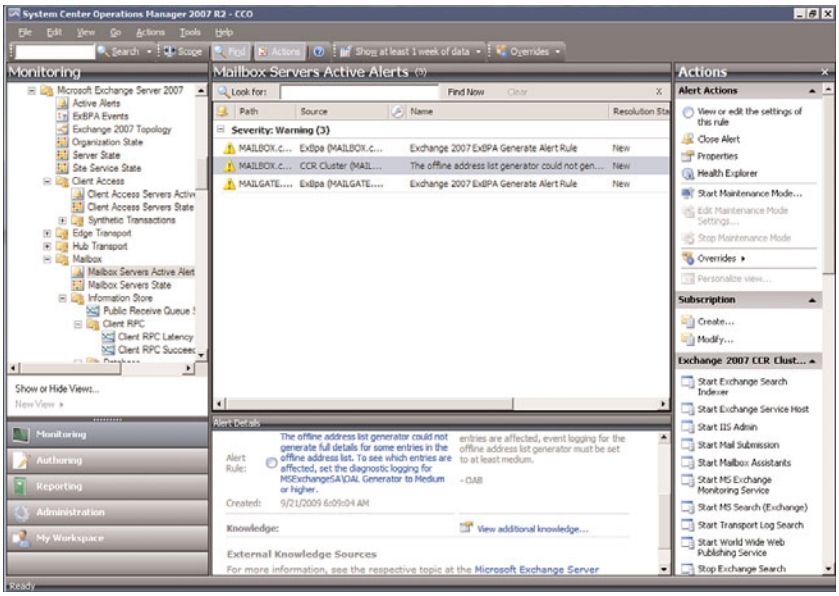

FIGURE 1.5 System monitoring and alerting in SCOM of specific servers in an environment.

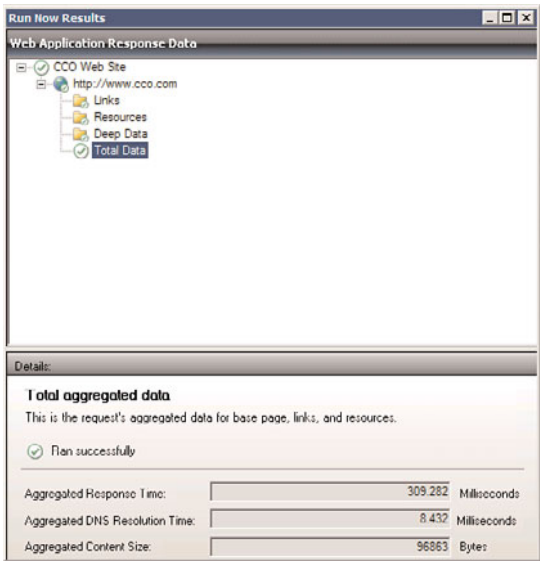

FIGURE 1.6 Monitoring applications and web URLs in SCOM.

- **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.

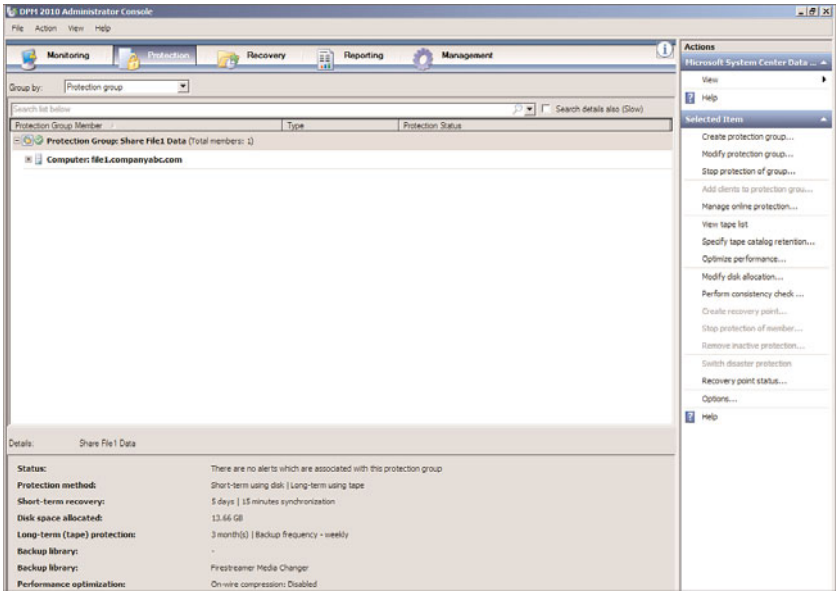

FIGURE 1.7 The System Center Data Protection Manager 2010 console.

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

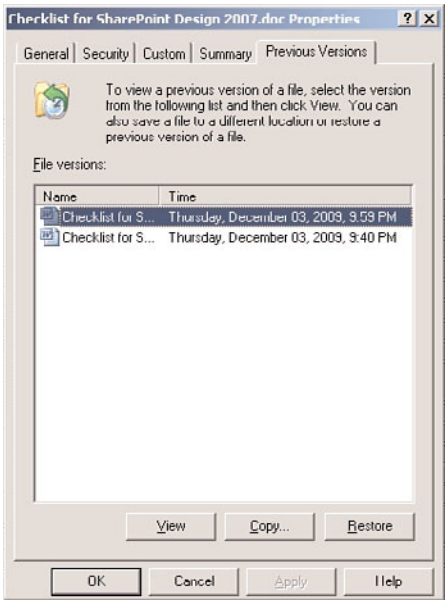

FIGURE 1.8 Self-service recovery of files leveraging DPM.

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 restoral of the information. The information from the recovery page of the console is shown in Figure 1.9.

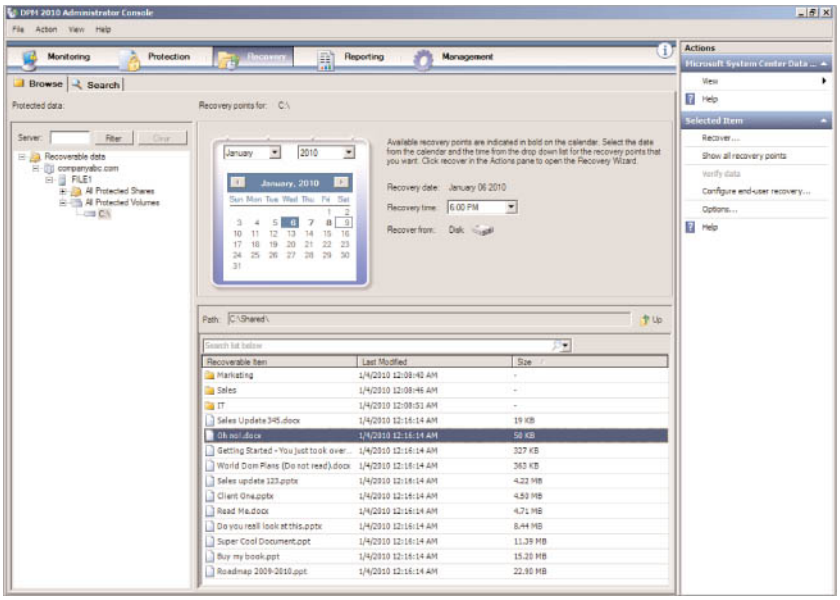

FIGURE 1.9 Recovery page from the DPM 2010 console.

- **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.

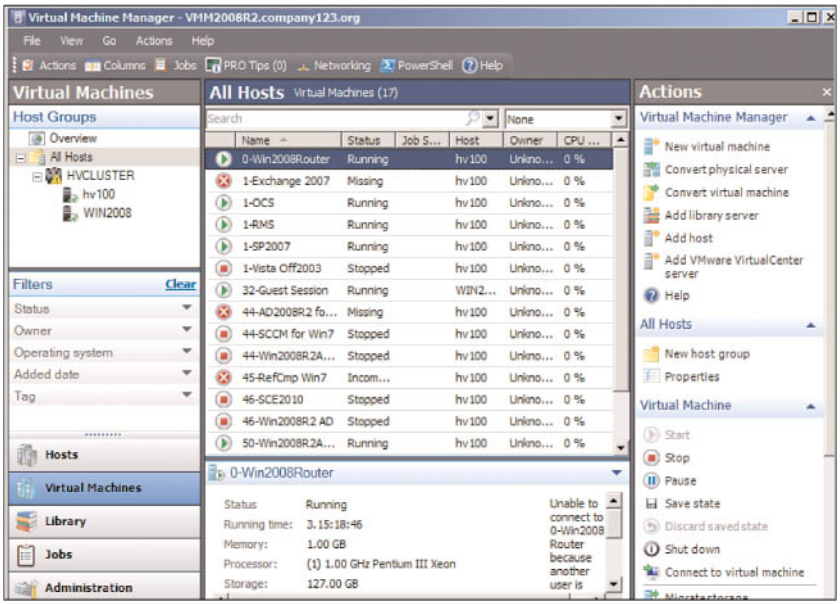

FIGURE 1.10 System Center Virtual Machine Manager console.

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.

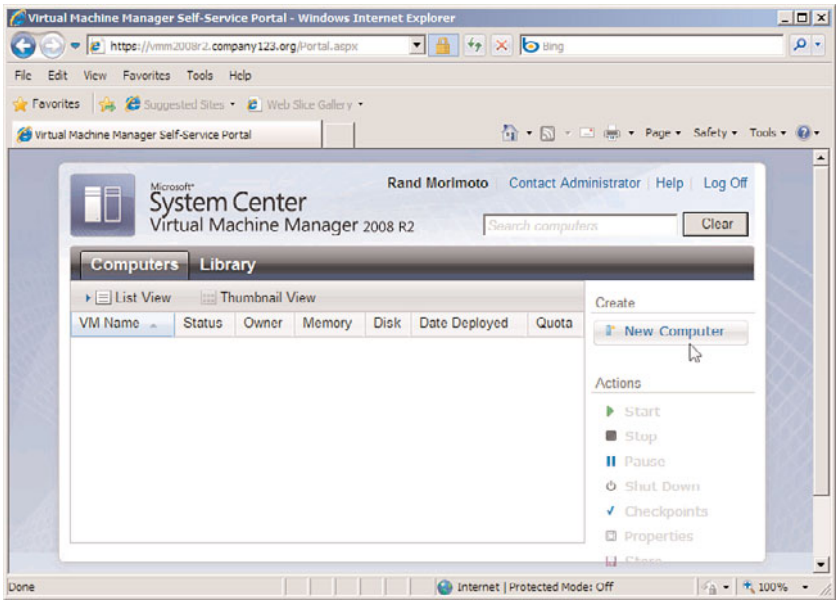

FIGURE 1.11 Self-service creation of guest sessions in VMM.

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.

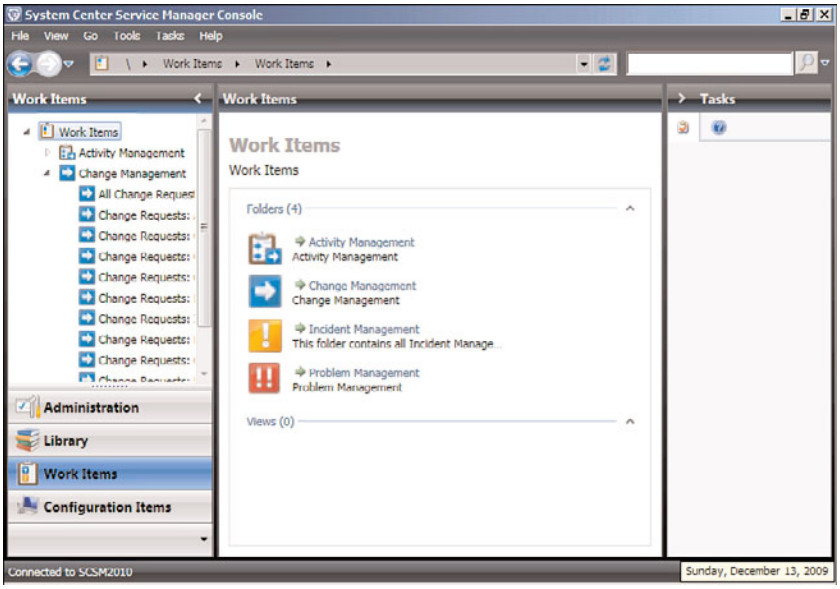

FIGURE 1.12 System Center Service Manager console.

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

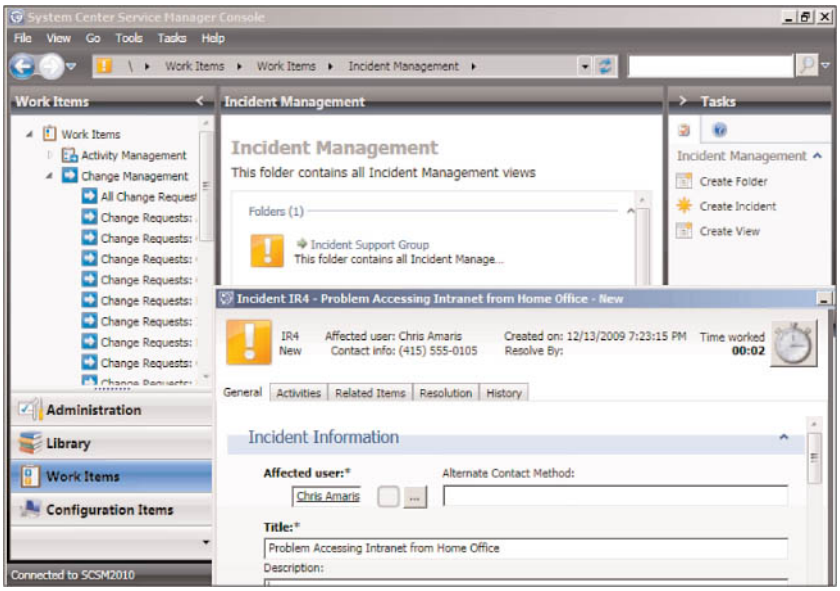

FIGURE 1.13 Incident management within SCSM.

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.

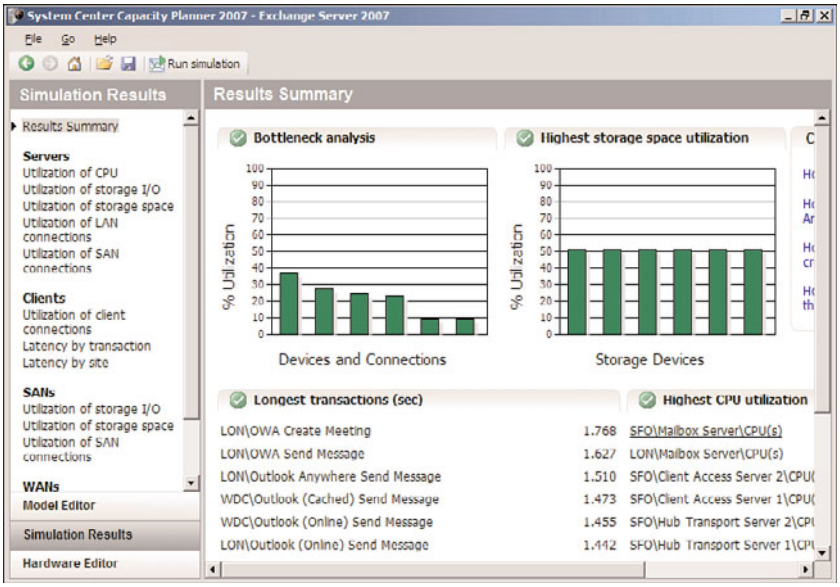

FIGURE 1.15 Simulation results report out of System Center Capacity Planner 2007.

- **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.

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.

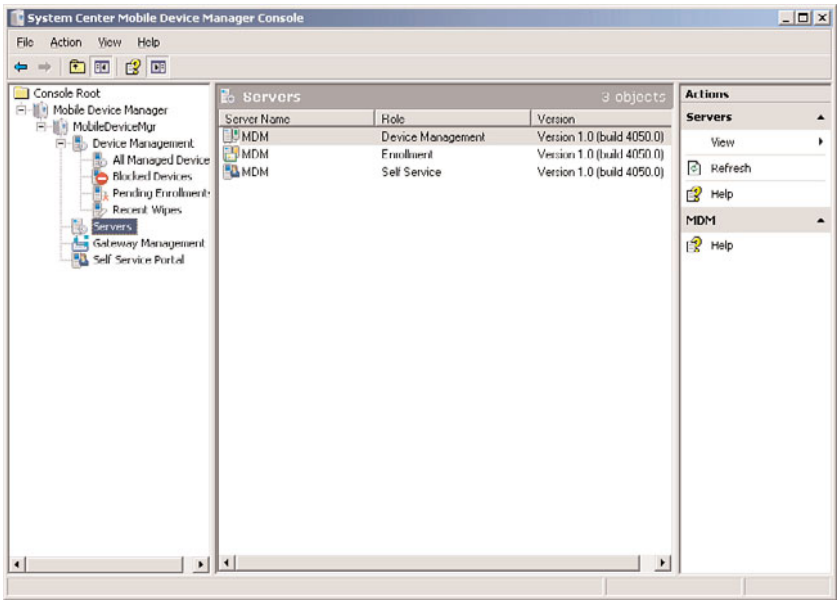

FIGURE 1.16 System Center Mobile Device Manager console.

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.

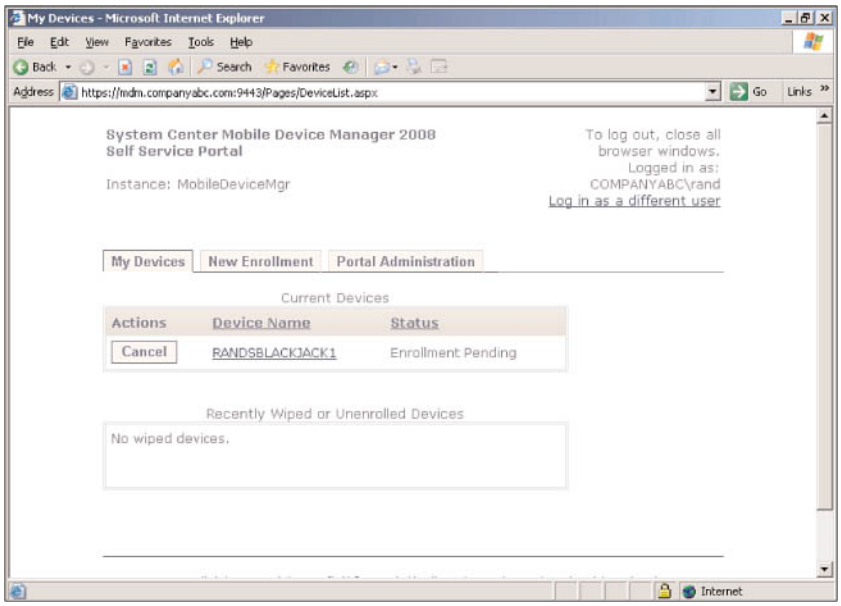

FIGURE 1.17 Self-service enrollment capabilities of MDM.

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 midsized 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.

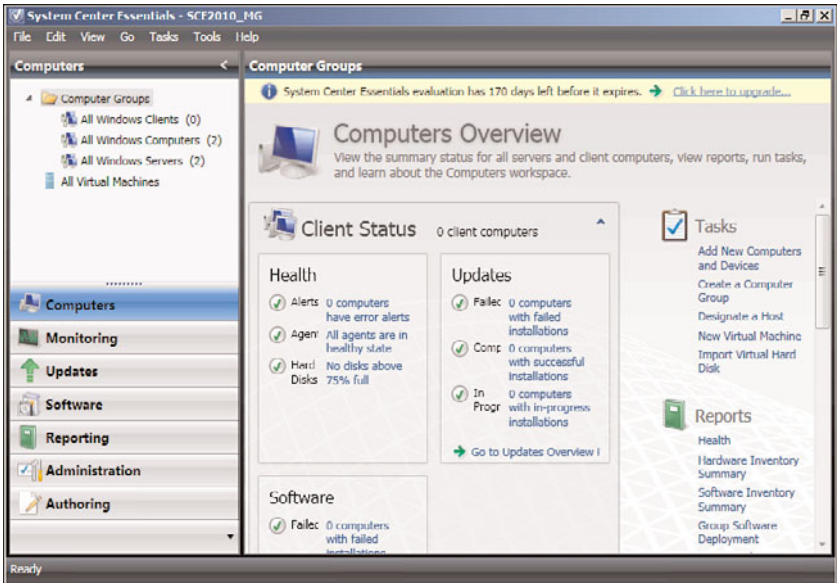

FIGURE 1.18 System Center Essentials console.

Business Solutions Addressed by System Center Essentials

For midsized 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 administer 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 midsized 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.

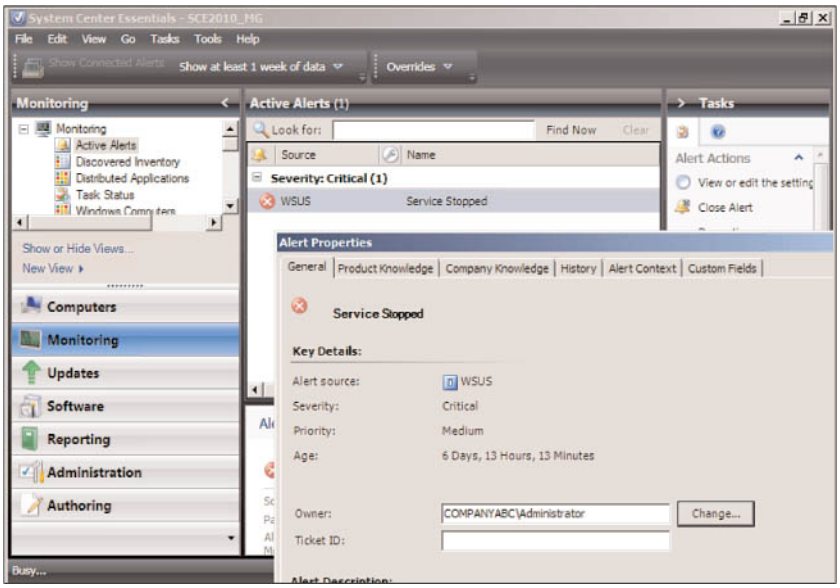

FIGURE 1.19 Server monitoring in System Center Essentials.

- **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

B

C

D

E

F

G

H

I

J-K

L

M

N

O

P

R

S

T

U

V

W