Contents at a Glance

Introduction ................................................................................... 1
1 Overview of the System Center Suite ................................................... 5
2 Configuration Manager 2012 Design and Planning .............................. 55
3 Configuration Manager 2012 Implementation and Administration ........ 115
4 Using Configuration Manager 2012 to Distribute Applications, Updates, and Operating Systems ..................................................... 181
5 Using Configuration Manager 2012 for Asset Management and Reporting .................................................................................... 245
6 Operations Manager 2012 Design and Planning ................................ 289
7 Operations Manager 2012 Implementation and Administration ........... 355
8 Using Operations Manager 2012 for Monitoring and Alerting .............. 421
9 Using Operations Manager 2012 for Operations and Security Reporting .................................................................................... 511
10 Data Protection Manager 2012 Design, Planning, Implementation, and Administration ................................................................. 567
11 Using Data Protection Manager 2012 to Protect File Systems, Exchange, SQL, and SharePoint ...................................................... 619
12 Virtual Machine Manager 2012 Design, Planning, and Implementation .................................................................................... 663
13 Managing a Hyper-V Environment with Virtual Machine Manager 2012 .................................................................................... 703
14 Service Manager 2012 Design, Planning, and Implementation ............. 761
15 Using Service Manager 2012 for Incident Tracking and Help Desk Support .................................................................................... 819
16 Using Service Manager 2012 for Service Offerings and Change Control Management .................................................................................... 871
17 System Center Orchestrator 2012 Design, Planning, and Implementation .................................................................................... 921
Index ......................................................................................... 969
# Table of Contents

## Introduction

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Overview of the System Center Suite</td>
<td>5</td>
</tr>
<tr>
<td>What Is System Center?</td>
<td>6</td>
</tr>
<tr>
<td>Understanding System Center Configuration Manager</td>
<td>9</td>
</tr>
<tr>
<td>Understanding System Center Operations Manager</td>
<td>18</td>
</tr>
<tr>
<td>Understanding System Center Data Protection Manager</td>
<td>26</td>
</tr>
<tr>
<td>Understanding System Center Virtual Machine Manager</td>
<td>34</td>
</tr>
<tr>
<td>Understanding System Center Service Manager</td>
<td>40</td>
</tr>
<tr>
<td>Understanding System Center 2012 Orchestrator</td>
<td>45</td>
</tr>
<tr>
<td>Understanding System Center Licensing</td>
<td>50</td>
</tr>
<tr>
<td>Summary</td>
<td>51</td>
</tr>
<tr>
<td>Best Practices</td>
<td>52</td>
</tr>
</tbody>
</table>

## Configuration Manager 2012 Design and Planning

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What’s New in ConfigMgr 2012</td>
<td>56</td>
</tr>
<tr>
<td>Explaining How Configuration Manager Works</td>
<td>60</td>
</tr>
<tr>
<td>Understanding Content Distribution</td>
<td>66</td>
</tr>
<tr>
<td>Understanding Asset Management</td>
<td>70</td>
</tr>
<tr>
<td>Reporting from Configuration Manager</td>
<td>74</td>
</tr>
<tr>
<td>Configuration Manager Architecture Components</td>
<td>75</td>
</tr>
<tr>
<td>Securing Configuration Manager</td>
<td>88</td>
</tr>
<tr>
<td>Understanding Component Requirements</td>
<td>92</td>
</tr>
<tr>
<td>Configuration Manager Design Considerations</td>
<td>94</td>
</tr>
<tr>
<td>Understanding Client Schedules</td>
<td>105</td>
</tr>
<tr>
<td>Planning for Internet-Based Client Management</td>
<td>106</td>
</tr>
<tr>
<td>Putting It All Together in a Design</td>
<td>110</td>
</tr>
<tr>
<td>Summary</td>
<td>112</td>
</tr>
<tr>
<td>Best Practices</td>
<td>112</td>
</tr>
</tbody>
</table>

## Configuration Manager 2012 Implementation and Administration

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample Organization</td>
<td>115</td>
</tr>
<tr>
<td>Configuring Installation Prerequisites</td>
<td>118</td>
</tr>
<tr>
<td>Implementing the Central Administration Site</td>
<td>124</td>
</tr>
<tr>
<td>Deploying the Primary Sites</td>
<td>129</td>
</tr>
<tr>
<td>Deploying the Secondary Sites</td>
<td>134</td>
</tr>
<tr>
<td>Configuring the Hierarchy</td>
<td>138</td>
</tr>
</tbody>
</table>
4 Using Configuration Manager 2012 to Distribute Applications, Updates, and Operating Systems
   Understanding Content Distribution .......................................................... 181
   Defining Collections ........................................................................... 185
   Understanding Application Management ................................................. 189
   Managing Deployments ........................................................................ 203
   Understanding Software Updates ........................................................... 215
   Deploying Software Updates ................................................................. 219
   Understanding Operating System Deployment ......................................... 225
   Deploying Operating Systems ................................................................. 234
   Extending with Microsoft Deployment Toolkit ......................................... 238
   Summary ............................................................................................ 243
   Best Practices .................................................................................... 243

5 Using Configuration Manager 2012 for Asset Management and Reporting
   Understanding Asset Data ..................................................................... 246
   Configuring Client Settings for Inventory Collection .............................. 248
   Understanding Reporting ...................................................................... 249
   Customizing Hardware Inventory .......................................................... 261
   Understanding Asset Intelligence ............................................................ 269
   Understanding Software Metering ........................................................... 277
   Understanding Compliance Settings ......................................................... 278
   Monitoring the Baselines and Compliance ................................................. 283
   Summary ............................................................................................ 285
   Best Practices .................................................................................... 285

6 Operations Manager 2012 Design and Planning
   What’s New With Operations Manager 2012 ........................................... 290
   Understanding How OpsMgr Works ........................................................ 291
   OpsMgr Architecture Components ......................................................... 296
   Securing OpsMgr .................................................................................. 311
   Fault Tolerance and Disaster Recovery .................................................... 317
   Understanding OpsMgr Component Requirements ..................................... 323
   OpsMgr Design Considerations ............................................................... 328
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>7  Operations Manager 2012 Implementation and Administration</td>
<td>355</td>
</tr>
<tr>
<td>Installing Operations Manager 2012</td>
<td>356</td>
</tr>
<tr>
<td>Deploying OpsMgr Agents</td>
<td>373</td>
</tr>
<tr>
<td>Monitoring DMZ Servers with Certificates</td>
<td>385</td>
</tr>
<tr>
<td>Configuring Operations Manager 2012</td>
<td>393</td>
</tr>
<tr>
<td>Administering Operations Manager 2012</td>
<td>403</td>
</tr>
<tr>
<td>Backing Up OpsMgr 2012</td>
<td>411</td>
</tr>
<tr>
<td>Summary</td>
<td>418</td>
</tr>
<tr>
<td>Best Practices</td>
<td>418</td>
</tr>
<tr>
<td>8  Using Operations Manager 2012 for Monitoring and Alerting</td>
<td>421</td>
</tr>
<tr>
<td>Using OpsMgr Consoles</td>
<td>422</td>
</tr>
<tr>
<td>Working with Management Packs</td>
<td>425</td>
</tr>
<tr>
<td>Exploring the Operations Manager Management Pack</td>
<td>432</td>
</tr>
<tr>
<td>Exploring the Windows Management Pack</td>
<td>440</td>
</tr>
<tr>
<td>Exploring the Active Directory Management Pack</td>
<td>451</td>
</tr>
<tr>
<td>Exploring the Exchange 2010 Management Pack</td>
<td>466</td>
</tr>
<tr>
<td>Exploring the SQL Server Management Pack</td>
<td>478</td>
</tr>
<tr>
<td>Exploring the Cross Platform Management Packs</td>
<td>487</td>
</tr>
<tr>
<td>Management Pack Templates</td>
<td>491</td>
</tr>
<tr>
<td>Custom Management Packs</td>
<td>503</td>
</tr>
<tr>
<td>Summary</td>
<td>508</td>
</tr>
<tr>
<td>Best Practices</td>
<td>508</td>
</tr>
<tr>
<td>9  Using Operations Manager 2012 for Operations and Security Reporting</td>
<td>511</td>
</tr>
<tr>
<td>Reporting from OpsMgr</td>
<td>512</td>
</tr>
<tr>
<td>Generating and Scheduling Reports</td>
<td>514</td>
</tr>
<tr>
<td>OpsMgr 2012 Maintenance Reports</td>
<td>532</td>
</tr>
<tr>
<td>Audit Collection Services Reporting</td>
<td>541</td>
</tr>
<tr>
<td>Service Level Tracking</td>
<td>548</td>
</tr>
<tr>
<td>OpsMgr 2012 Dashboards</td>
<td>554</td>
</tr>
<tr>
<td>Publishing Dashboards into SharePoint 2010</td>
<td>561</td>
</tr>
<tr>
<td>Summary</td>
<td>565</td>
</tr>
<tr>
<td>Best Practices</td>
<td>566</td>
</tr>
</tbody>
</table>
10 Data Protection Manager 2012 Design, Planning, Implementation, and Administration

What Is System Center Data Protection Manager? .............................. 568
Data Protection Manager Background .............................................. 572
Data Protection Manager Prerequisites ............................................. 578
Planning a Data Protection Manager Deployment .............................. 580
Deploying Data Protection Manager ................................................ 587
Completing Required Configuration Tasks ........................................ 591
Creating Protection Groups ............................................................ 601
Administrating Data Protection Manager .......................................... 606
Summary .................................................................................... 616
Best Practices ............................................................................... 617

11 Using Data Protection Manager 2012 to Protect File Systems,
Exchange, SQL, and SharePoint

Protecting File Servers................................................................... 620
Protecting System State ................................................................. 622
Protecting Exchange Servers ........................................................... 624
Protecting SQL Servers................................................................... 635
Protecting SharePoint Farms ........................................................... 643
Protecting Virtualized Environments............................................... 654
Summary .................................................................................... 660
Best Practices ............................................................................... 661

12 Virtual Machine Manager 2012 Design, Planning, and Implementation

Understanding Virtual Machine Manager ......................................... 663
Virtual Machine Manager Background ............................................. 673
What’s New in System Center Virtual Machine Manager 2012 .......... 677
Virtual Machine Manager Prerequisites ............................................ 678
Planning a Virtual Machine Manager Deployment ............................. 682
Deploying Virtual Machine Manager ............................................... 687
Summary .................................................................................... 700
Best Practices ............................................................................... 701

13 Managing a Hyper-V Environment with Virtual Machine Manager 2012

Understanding the VMM Private Cloud ........................................... 704
Using the VMM Management Interfaces .......................................... 707
Understanding Virtual Machine Conversions .................................... 716
Managing VMM User Roles ............................................................ 729
Deploying Virtual Machines ........................................................... 740
Migrating Virtual Machines ............................................................ 747
# Understanding and Implementing Server App-V

- 753

## Summary

- 758

## Best Practices

- 759

# 14 Service Manager 2012 Design, Planning, and Implementation

- 761

1. What's New in Service Manager 2012

- 762

2. Explaining How Service Manager Works

- 763

3. Service Manager Design Parameters

- 769

4. Putting It All Together in a Service Manager Design

- 775

5. Planning a Service Manager Deployment

- 783

6. Deploying Service Manager

- 791

7. Deploying Service Manager Connectors

- 805

8. Backing Up Service Manager 2012

- 814

## Summary

- 817

## Best Practices

- 817

# 15 Using Service Manager 2012 for Incident Tracking and Help Desk Support

- 819

1. Incidents and Problems

- 819

2. Configuring Incident Settings

- 821

3. Service Manager Notifications

- 830

4. Creating New Incidents

- 836

5. Working with Incidents

- 846

6. Configuring Problem Settings

- 856

7. Working with Problems

- 859

8. Incident and Problem Reports

- 863

## Summary

- 869

## Best Practices

- 870

# 16 Using Service Manager 2012 for Service Offerings and Change Control Management

- 871

1. Service Manager 2012 and the Infrastructure Optimization Model

- 871

2. Service Offerings and Request Offerings in SM 2012

- 872

3. Release Management in SM 2012

- 882

4. Change Requests and Activities

- 885

5. Configuring Change Settings

- 887

6. Change Management Templates and Workflows

- 889

7. Initiating Change Requests

- 892

8. Working with and Approving Change Requests

- 896

9. Implementing Change Requests

- 903

10. Managing Configuration Items

- 910
# Contents

Working with Change, Activity, and Configuration Management

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports</td>
<td>914</td>
</tr>
<tr>
<td>Summary</td>
<td>919</td>
</tr>
<tr>
<td>Best Practices</td>
<td>920</td>
</tr>
</tbody>
</table>

## 17 System Center Orchestrator 2012 Design, Planning, and Implementation

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of System Center Orchestrator</td>
<td>921</td>
</tr>
<tr>
<td>History of System Center Orchestrator</td>
<td>924</td>
</tr>
<tr>
<td>System Center Orchestrator 2012 Installation Prerequisites</td>
<td>924</td>
</tr>
<tr>
<td>Orchestrator Security Planning</td>
<td>926</td>
</tr>
<tr>
<td>Installing System Center Orchestrator 2012 on a Single Server</td>
<td>928</td>
</tr>
<tr>
<td>Installing System Center Orchestrator 2012 on Separate Systems</td>
<td>933</td>
</tr>
<tr>
<td>Additional Tasks Following Orchestrator Installation</td>
<td>939</td>
</tr>
<tr>
<td>Getting Familiar with the Orchestrator 2012 Management Consoles</td>
<td>942</td>
</tr>
<tr>
<td>Installing Integration Packs</td>
<td>949</td>
</tr>
<tr>
<td>Designing and Using Runbooks</td>
<td>952</td>
</tr>
<tr>
<td>Runbook Permissions</td>
<td>967</td>
</tr>
<tr>
<td>Summary</td>
<td>967</td>
</tr>
<tr>
<td>Best Practices</td>
<td>968</td>
</tr>
</tbody>
</table>

## Index

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>969</td>
</tr>
</tbody>
</table>
About the Authors

Chris Amaris, MCITP, MCTS, CISSP/ISSAP, CHS III, is the chief technology officer and cofounder of Convergent Computing. He has more than 20 years experience consulting for Fortune 500 companies, leading companies in the technology selection, design, planning, and implementation of complex information technology projects. Chris has worked with Microsoft System Center products, such as Operations Manager and Configuration Manager, since their original releases in 2000 and 1994. He specializes in messaging, security, performance tuning, systems management, and migration. Receiving his first Microsoft technologies certification in 1993, Chris is a current Microsoft Certified IT Professional (MCITP) with multiple Microsoft Certified Technology Specialist designations (MCTS) in System Center technologies, a Certified Information Systems Security Professional (CISSP) with an Information System Security Architecture Professional (ISSAP) concentration, Certified Homeland Security (CHS III), a Novell CNE, a Banyan CBE, and a Certified Project Manager. Chris is also an author, writer, and technical editor for a number of IT books, including *Network Security for Government and Corporate Executives*, *Exchange 2010 Unleashed*, and *Microsoft Windows Server 2008 R2 Unleashed*.

Rand Morimoto, Ph.D., MVP, MCITP, CISSP, has been in the computer industry for over 30 years and has authored, coauthored, or been a contributing writer for dozens of books on Windows, Security, Exchange, BizTalk, and Remote and Mobile Computing. Rand is the president of Convergent Computing, an IT-consulting firm in the San Francisco Bay area that has been one of the key early adopter program partners with Microsoft, implementing the latest Microsoft technologies, including Microsoft Windows Server 2008 R2, System Center 2012, Windows 7, Exchange Server 2010, Windows Server 2012, and SharePoint 2010 in production environments over 18 months before the initial product releases.

Pete Handley, MCITP, CISSP, has more than 15 years of experience in IT, including extensive knowledge of Active Directory, Microsoft Exchange, Windows Server 2008, and the System Center suite of products. He has been a contributing author for the Sams books *Microsoft Exchange 2003 Unleashed* and *Windows PowerShell Unleashed*. Pete specializes in Visual Basic and PowerShell scripting and is a subject matter expert on the integration and migration of Novell technologies to Microsoft technologies. Pete holds the Microsoft Certified Systems Engineer 2003 (MCSE) certification, the Microsoft Certified Information Technology Professional (MCITP) certification, the Novell Certified Directory Engineer (CDE) certification, and the Certified Information Systems Security Professional (CISSP) certification.
David E. Ross, MCITP, VCP, CCEA, CCSP, has over 13 years of experience in IT consulting, the majority of which have been spent playing the lead architect role on network design and implementation projects throughout the San Francisco Bay area. David is currently acting as a principal engineer for Convergent Computing, and is frequently involved in creating hybrid solutions involving multiple vendor technologies for organizations of all sizes. Specialties for David include Active Directory, Exchange, System Center, Lync, Citrix XenApp and XenDesktop design, virtualization solutions using VMware vSphere and Microsoft Hyper-V, and Cisco routing, switching, and security technologies.
Dedication

I dedicate this book to my wife Sophia, light of my life. And to my children, Michelle, Megan, Zoe, Zachary, and Ian, who give meaning to my life and work.

—Chris Amaris, MCITP, MCTS, CISSP/ISSAP, CHS III

I dedicate this book to Ana, looking forward to continuing a wonderful life together!

—Rand Morimoto, Ph.D., MVP, MCITP, CISSP

I dedicate this book to my parents Hal and Denise, who encouraged my early love of reading and gave me my first computer. You have each made it possible for me to learn and grow in so many ways, but the greatest lessons that I have learned have been by your examples. And to my wonderful and irrepressible wife Melissa, you are the joy at the center of my life and never far from my thoughts.

—Pete Handley, MCITP, CISSP

I dedicate this book to my wife Lisette, who serves as an inspiration to everyone around her, and encourages everyone to reach their full potential. Thanks for your loving support during this project, and for the sacrifices you made to help me reach my potential. Also to my fun-loving boys Caden and Cole, who keep me on my toes and provide the best distraction from long hours of book writing. Thanks for being a great family worth working hard for!

—David E. Ross, MCITP

I dedicate this book to everyone at Convergent Computing. Credit for the book should be spread throughout the entire organization for an effort that would be largely impossible without the contribution of the whole team.

—Guy Yardeni, MCSE, MCITP, CISSP
Acknowledgments

Chris Amaris, MCSE, MVP, CISSP
I want to thank Rand for providing the leadership and direction as we have transitioned from a server centric focus, to enterprise data center centric focus, to now a cloud centric focus. Your vision on the IT industry needs, trends, and technologies has allowed you to keep a steady hand on the tiller, ensuring that we are always ahead of the latest technology wave. The breadth and depth of knowledge of the Convergent Computing organization in the System Center technologies that allow us to support our clients and provide the basis for this book are all thanks to your vision and leadership.

And many, many thanks to my family! Sophia, thank you for keeping everything together while I disappeared at the drop of a hat into my office to finish another lab or chapter. Michelle, Megan, Zoe, Zachary, and Ian, thank you for keeping focused on your academics and seeing that through hard work anything is possible.

Rand Morimoto, Ph.D., MVP, MCITP, CISSP
Congratulations Chris for getting this System Center 2012 title out the door! And a big thanks to Pete and Dave who jumped in to the middle of this book, GREAT job in rounding out the authoring team on this one! And a huge thanks to Guy for doing the edits and making sure this book was prime time!

I want to thank the team at Sams Publishing for continuing to support our writing efforts and turning this book around and out to print in record time! Thank you Neil, Mark, Andy, and all the folks behind the scenes in making this happen! And my thanks to Karen Annett, who continues to be my favorite copy editor!!!

I also wanted to thank the consultants at Convergent Computing and our early adopter clients who fiddle with these new technologies really early on and then take the leap of faith in putting the products into production to experience (and at times feel the pain) as we work through best practices. The early adopter experiences give us the knowledge and experience we need to share with all who use this book as their guide in their production environments based on the lessons learned.

To Kelly, Noble, and Chip, yeah, one down, three more books to go before the year is up. You know where to find me in the wee hours of the night, downstairs at the kitchen table writing. Remember to work hard at everything you do, as you’ve found so far, you can accomplish a lot when you put your mind to things!

Pete Handley, MCITP, CISSP
I want to thank Rand for the opportunity to contribute to this book, and to Chris for your thorough and patient approach to learning. Thanks to Guy for your meticulous tech editing, and to Karen and the SAMS team for always sweating the details!
David E. Ross, MCITP
Thanks to my family for the sacrifices they made without complaint while I was getting oriented with the whole book-authoring process. Big thanks also to Rand not only for providing me the opportunity to work on this project, but for providing excellent guidance on the whole process. You made it very easy to come up to speed and learn the ropes very quickly; I appreciate it!
We Want to Hear from You!

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

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

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

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

E-mail: feedback@samspublishing.com

Mail: Neil Rowe  
Executive Editor  
Sams Publishing  
800 East 96th Street  
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at informit.com/register for convenient access to any updates, downloads, or errata that might be available for this book.
This page intentionally left blank
Introduction

The release of System Center 2012 is a major shift in the System Center family of products of going from a product line that was previously sold and viewed as a series of individual products, to System Center 2012 being sold as a single product with tight integration between the various components. In addition, this shift is not just from the perspective of a sales or marketing focus of a single product, but also from the engineering integration of System Center 2012 where the components work better and tighter together.

Additionally, with System Center 2012, Microsoft has expanded beyond the traditional “only Microsoft” solution support to one that broadly embraces other platforms, such as the support for VMware, Citrix, storage area network products from various vendors, non-Microsoft mobile devices and operating systems, and the like. From a data center perspective where the data center has more than just Windows servers and Microsoft applications, this multivendor support is critical in Microsoft’s ability to be a true data center management solution provider.

And as the industry evolves to support traditional on-premise servers and applications and now cloud-based products and technologies, System Center’s ability to support applications and services in the cloud is a critical inclusion in the System Center 2012 product.

This book covers real-world experiences with System Center 2012, 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 17 chapters of this book are written to highlight the most important aspects of the technologies that make up the System Center family of components. To combine the components into groups of technologies, this book covers the following:

- **Introduction**—The first chapter of this book provides an introduction to the System Center 2012 family of components, 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 covers 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 2012 Configuration Manager**—The first component covered in this book is the System Center 2012 Configuration Manager (SCCM) component, which is a toolset 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 four or five generations later, SCCM 2012 has really helped organizations with the patching, updating, imaging, reporting, and compliance management of their systems, both Microsoft and non-Microsoft endpoint clients and servers. 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 component, and, more important, how administrators use SCCM to image, update, manage, and support the servers and client systems in their environments.

- **System Center 2012 Operations Manager**—The second component covered in this book is the System Center 2012 Operations Manager (SCOM) component, which provides monitoring and alerting on servers and client systems as well as internetworking devices (routers/switches/firewalls) and cloud-based services. Rather than waiting for users to alert the help desk that a server is down, SCOM proactively monitors systems and networks and provides alerts before failures impact operations, 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 environments.

- **System Center 2012 Data Protection Manager**—System Center 2012 Data Protection Manager (DPM) is a relatively new addition to the Microsoft management family of components. 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, SQL, Hyper-V hosts and guests, and Windows client systems using DPM 2012.

- **System Center 2012 Virtual Machine Manager**—In the past three to four 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 four major updates to the System Center Virtual Machine Manager (VMM) component in three years to address the needs of the enterprise. The two chapters dedicated to VMM go beyond the installation and setup of VMM 2012, and get into core components of the component that help organizations manage virtual guest sessions running on Microsoft Hyper-V, VMware, and Citrix XenServer, and also how to convert physical servers to virtual servers (P2V), delegate the ability to administer and manage guest sessions, manage the “fabric” of a network (storage and internetworking), and the ability to share virtual host resources with users and administrators in the enterprise.
System Center 2012 Service Manager—After an initial five years in development and over two years in production deployments, Microsoft now has a help desk/incident management/asset life-cycle management/change management component called System Center 2012 Service Manager (SCSM) that organizations are finding extremely valuable in their enterprises. 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 component. SCSM brings together the information gathering, reporting, alerting, and knowledge-base information in the other System Center components into a single component that will help organizations better manage their IT infrastructures.

System Center 2012 Orchestrator—System Center Orchestrator is a newcomer to the System Center family and has been instrumental in real-world implementations of System Center in helping to make process and runbook automated tasks that simplify IT processes. For tasks that IT professionals have manually done day in and day out in the past that takes hours or days to complete, Orchestrator scripts run through the processes methodically in minutes and seconds. The consistency with Orchestrator scripts helps organizations maintain standards and consistency in processes and achieve end goals more efficiently and effectively than in the past.

It is our hope that the real-world experience we have had in working with the entire System Center family of components 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 management tools from Microsoft!
This page intentionally left blank
IN THIS CHAPTER

Sample Organization
Configuring Installation Prerequisites
Implementing the Central Administration Site
Deploying the Primary Sites
Deploying the Secondary Sites
Configuring the Hierarchy
Configuring Sites
Configuring Client Settings
Implementing Internet-Based Client Management
Best Practices

CHAPTER 3
Configuration Manager 2012 Implementation and Administration

System Center Configuration Manager (ConfigMgr) 2012 helps reduce the cost of managing the Windows infrastructure by providing scalable, secure, end-to-end administration and reporting functionality for the enterprise. It is important to fully understand the architectural design before Configuration Manager 2012 infrastructure servers and roles are deployed.

This chapter walks through the steps necessary to deploy, configure, and administer key Configuration Manager 2012 functionality. This functionality includes deploying and administering the roles and features needed to enable operating system deployment, systems configuration management, patch management, software provisioning, asset management, and reporting.

Sample Organization
To illustrate the implementation and administration of Configuration Manager 2012, a multilocation sample organization named Company XYZ will be used. This will provide a backdrop of reality against which the Configuration Manager 2012 design can be developed.

Existing Environment
Company XYZ is headquartered in San Francisco with offices in Paris, London, Tokyo, and New York City. The company has over 3,000 employees distributed primarily between San Francisco and Paris. London and Tokyo are
medium-sized branch offices. Finally, the New York office is a very small office with only a handful of employees.

There is a network connection between the San Francisco and Paris offices. London and Tokyo connect to the Paris office. New York is connected to the separate San Francisco office. Figure 3.1 shows the corporate wide area network (WAN) topology.

The company has a single Active Directory forest and domain. The domain name is companyxyz.com and has a domain controller DC1. Each office has its own Active Directory site in the Active Directory site topology. Table 3.1 summaries the location information.

<table>
<thead>
<tr>
<th>Location</th>
<th>AD Site</th>
<th>Network</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>San Francisco</td>
<td>SFO</td>
<td>10.1.x.x</td>
<td>2,000</td>
</tr>
<tr>
<td>Paris</td>
<td>PAR</td>
<td>10.4.x.x</td>
<td>1,000</td>
</tr>
<tr>
<td>London</td>
<td>LON</td>
<td>10.2.x.x</td>
<td>100</td>
</tr>
<tr>
<td>Tokyo</td>
<td>TOK</td>
<td>10.5.x.x</td>
<td>100</td>
</tr>
<tr>
<td>New York</td>
<td>NYC</td>
<td>10.3.x.x</td>
<td>5</td>
</tr>
</tbody>
</table>

The San Francisco office has the central IT organization that covers the entire Company XYZ organization, but the Paris office also has a smaller IT organization that covers the Paris, London, and Tokyo locations. The Paris office has significant autonomy and needs administrative control over its infrastructure due to regulatory concerns.

This information will be used to inform the Configuration Manager 2012 design.
Developing a Configuration Manager 2012 Design

Based on the Company XYZ existing environment, the recommendation would be to have a Primary Site Server in San Francisco and a Primary Site Server in Paris based on the local IT presence and the requirement for local administrative control. The recommendation would be to place Secondary Site Servers in London and Tokyo based on the size of the offices. Given the small size of the New York office with only five users, no servers will be placed there.

Table 3.2 summarizes the locations, server roles, and server names needed for the infrastructure.

<table>
<thead>
<tr>
<th>Location</th>
<th>SCCM Site</th>
<th>Site Code</th>
<th>Server Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>San Francisco</td>
<td>Central Administration Site</td>
<td>XYZ</td>
<td>CM1</td>
</tr>
<tr>
<td></td>
<td>Primary Site</td>
<td>SFO</td>
<td>CM2</td>
</tr>
<tr>
<td>Paris</td>
<td>Primary Site</td>
<td>PAR</td>
<td>CM3</td>
</tr>
<tr>
<td>London</td>
<td>Secondary Site</td>
<td>LON</td>
<td>CM4</td>
</tr>
<tr>
<td>Tokyo</td>
<td>Secondary Site</td>
<td>TOK</td>
<td>CM5</td>
</tr>
<tr>
<td>New York</td>
<td></td>
<td>NYC</td>
<td></td>
</tr>
</tbody>
</table>

Figure 3.2 shows a diagram of the recommended Configuration Manager 2012 infrastructure.

The balance of this chapter implements and configures the Configuration Manager 2012 design for Company XYZ.
Configuring Installation Prerequisites

Before implementing SCCM 2012, several prerequisite steps need to be taken to prepare Active Directory and the Site Servers. These steps ensure that the SCCM implementation goes smoothly.

The required SCCM prerequisites are as follows:

- Extending the Active Directory schema
- Configuring the System Management container in Active Directory
- Adding Windows roles and features on Site Servers

These prerequisites prepare the environment for Configuration Manager 2012.

These installation prerequisites are in addition to the hardware and software requirements covered in Chapter 2, “Configuration Manager 2012 Design and Planning.” The software requirements include the following:

- Windows Server 2008 64-bit SP2 or Windows Server 2008 R2 operating system
- Windows Active Directory domain
- .NET Framework 3.51 SP1
- .NET Framework 4.0
- SQL Server 2008 SP2 with Cumulative Update 7 or SQL Server 2008 R2 SP1 with Cumulative Update 4 (can be on a separate server)
- Opened TCP port 1433 and 4022 for SQL replication

The hardware and software requirements for all prospective Site Servers must be met before the installation prerequisites can be configured.

NOTE

If you install IIS after installing .NET Framework 4.0, then open a command prompt, browse to the location %windir%\Microsoft.NET\Framework64\v4.0.30319, and execute aspnet_regiis.exe -i --enable.

Extending the Active Directory Schema

The Active Directory schema should be extended to support dynamic client assignment during Configuration Manager agent deployment and to assist clients with the location of Configuration Manager server infrastructure. When the Active Directory schema is extended, clients can use the values provided through Active Directory to locate regional Site Servers and Distribution Points for package and content delivery.
NOTE
The Active Directory schema extensions for SCCM 2012 are identical to the Active Directory schema extensions for SCCM 2007. If the schema was already extended for SCCM 2007, the schema does not need to be extended again for SCCM 2012.

CAUTION
Take the appropriate safety measures when extending the Active Directory schema. Changes to the schema cannot be easily reversed; plan to test the schema extensions in a development environment before implementing them in your production environment.

To extend the Active Directory schema, execute the following steps:

1. Log on to a domain controller with an administrative account that is a member of the Schema Admins group.
2. Copy the EXTADSCH.exe from \SMSSETUP\BIN\x64\ on the Configuration Manager installation media to a local folder on the Active Directory domain controller with the schema master FSMO role.
3. Open a command window as an administrator and execute the EXTADSCH.exe command with a Schema Admin account.

The command should report, “Successfully extended the Active Directory schema” when complete (as shown in Figure 3.3).

![Figure 3.3 Successful Active Directory schema extension.](image)

Review the ExtADSch.log file for any errors. This log file is located in the root of drive C on the server used to execute the schema extensions. The log file should show 14 attributes and four classes have been defined.
TIP

Sometimes, the attribute extensions will succeed, but the class extensions will fail. This is typically due to replication latency, especially in large distributed environments. The EXTADSDCH.exe command can be run multiple times with no ill effect. Wait for replication to complete and then run the schema extension command again. After replication is completed, the class extensions should be successful.

Configuring the System Management Container

When the Active Directory schema has been extended, Configuration Manager Site Servers store information about the hierarchy in special Active Directory objects. These objects are kept in a specific folder in the System container of the domain partition. The location for these objects doesn’t exist by default, and must be manually created and configured.

In a distributed Configuration Manager hierarchy, it is considered best practice to place the Configuration Manager Site Servers in a custom security group, and delegate this security group’s permissions to the System Management container in Active Directory. The following tasks assume the Configuration Manager Site Servers (CM1, CM2, CM3, CM4, and CM5) are members of the “SCCM Site Servers” universal security group. If this group doesn’t exist, create it before continuing.

CAUTION

When a computer object is added to a group, it can take a long time for the setting to take effect. This is because the Kerberos ticket takes seven days to renew. The renewal time is governed by the Maximum Lifetime for User Ticket Renewal setting located in the Default Domain Policy GPO. It is not recommended to change this setting. Instead, restart the computer to refresh the Kerberos ticket.

The System Management container holds the Configuration Manager objects in Active Directory. This container can be created with the ADSI Edit console on the DC1 domain controller.

To create the System Management container with ADSI Edit, complete the following steps:

1. Run ADSI Edit from DC1.
2. Right-click the ADSI Edit node and select Connect To.
3. Type Domain in the Name field.
4. Select Default Naming Context from the list of well-known naming contexts.
5. Click OK.
7. Expand DC=companyxyz,DC=com.
8. Select the CN=System container.
9. Right-click CN=System, click New, and then click Object.
10. Select Container from the list and click Next.
11. Enter **System Management** for the CN attribute value, and then click Next.
12. Click Finish to complete the change.

The permissions for the System Management container need to be configured before the first Site Server is implemented.

To set the System Management container permission with ADSI Edit, complete the following steps:

1. Right-click the System Management container and select Properties.
2. Select the Security tab.
3. Click Advanced.
4. Click Add.
5. Type **SCCM Site Servers** and click OK.
6. Continue with the default selection of This Object and All Descendant Objects from Apply To.
7. Choose Allow in front of Full Control in the Permissions field and then click OK.
8. Click OK two times to commit all the changes and then close ADSI Edit.

As Configuration Manager Site Servers are added to the hierarchy, be sure to add them to the custom Site Servers security group (SCCM Servers). This ensures they can create the required Active Directory objects.

**Adding Windows Roles and Features on Site Servers**

The majority of client communications is over HTTP or HTTPS, which is serviced by the Windows IIS web server. IIS is a key component of many Configuration Manager Site Systems roles. This includes the Site Server itself in the following optional roles:

- Application Catalog Web Service Point
- Application Catalog Website Point
- Distribution Point
- Enrollment Point
- Enrollment Proxy Point
NOTE

Some Configuration Manager 2012 Site System roles will require additional installation of Windows roles or features, such as for the software update point, which requires the Windows Server Update Services (WSUS) role, or Distribution Point, which requires IIS request filtering to be configured. These additional configurations will be done as part of configuring those Site System roles.

It is important to make sure that IIS is installed correctly on each of the Site Systems; otherwise, SCCM will not operate correctly.

To implement IIS on the Site Server and Component Servers on a Windows Server 2008 R2–based system, complete the following steps:

1. Open Server Manager on the Site/Component Server.
2. Select the Features node.
3. Click the Add Features action.
4. Enable Background Intelligent Transfer Service (BITS).
5. When prompted, click Add Required Role Services.

NOTE

Clicking the Add Required Role Services button automatically enables IIS and common related features required to host the Configuration Manager service. This includes Web Server components, Management Tools, and Remote Server Administration Tools.

7. On the Web Server Overview page, click Next.
8. Enable the ASP.NET role service, and click Add Required Role Services.
9. Enable the ASP role service.
10. Enable the Windows Authentication role service.
11. Enable the IIS 6 WMI Compatibility role service and the IIS 6 Metabase Compatibility if they are not already, and then click Next.
12. Review the components selected and click Install.

13. Close the wizard when the installation completes.

During this process, a number of roles, role services, and features get enabled automatically. If the preparation is being done on a system with some of these enabled or disabled, it can be confusing to know which ones need to be added.

To install using the command line, open Windows PowerShell as an administrator and enter the following commands:

```
Import-Module ServerManager
```

When the preparation process is completed, at minimum the Web Server (IIS) role should be installed with the following list of role services:

- Static Content
- Default Document
- Directory Browsing
- HTTP Errors
- HTTP Redirection
- ASP.NET
- .NET Extensibility
- ISAPI Extensions
- ISAPI Filters
- HTTP Logging
- Logging Tools
- Request Monitor
- Tracing
- Windows Authentication
- Request Filtering
- Static Content Compression
- Dynamic Content Compression
- IIS Management Console
- IIS 6 Metabase Compatibility
- IIS 6 WMI compatibility
In addition, the following Windows features should be installed:

- Background Intelligent Transfer Service (BITS)
- Remote Differential Compression
- Web Server (IIS) Tools
- BITS Server Extensions Tools

In preinstalled systems, ensure that the preceding role services and features are installed.

**Implementing the Central Administration Site**

The Configuration Manager Central Administration Site is the primary site located at the very top of the Configuration Manager hierarchy. This site is needed if there will be more than one primary site in the hierarchy.

There is a very important implementation difference between the Configuration Manager 2012 Central Administration Site and the central site in previous versions. In previous versions, Primary Site Servers can be installed and later connected to the central site. This is no longer possible in Configuration Manager 2012 and Primary Site Servers must be connected to their Central Administration Site during installation. This means that the Central Administration Site must be installed before any primary sites in the hierarchy.

The net result of these changes is that the Central Administration Site is required and must be the first site implemented if there will be more than one Primary Site Server in the hierarchy, as is the case in the sample Company XYZ architecture.

Verify that all of the hardware and software requirements have been met and that the installation configuration prerequisites have been completed.

**Installing the Central Administration Site Server**

Before running the Configuration Manager setup, run the prerequisite checker to verify the required components have been successfully installed. The prerequisite checker can be launched from a link on the splash.hta page. The splash.hta page can be found in the root of the Configuration Manager media.

**TIP**

Make sure the Configuration Manager Site Server Computer Account is in the local administrators group on all component servers and other Site Servers—this includes the Site Database server. The computer account of the Site Server is used to access and manage the remote server by default. One way to accomplish this is by creating a group named SCCM Site Servers with the computer accounts of all SCCM Site Servers as members and then adding that group to the Local Administrator group on all Site Servers.
Before starting the installation process, create a folder on the C: drive called “SCCMUpdates” and share this folder. This folder will store the latest prerequisite components downloaded during the installation process. This folder can be reused during subsequent Site Server installations.

To install the XYZ Central Administration Site Server on the CM1 server and establish the Company XYZ hierarchy, complete the following steps:

1. Launch splash.hta from the Configuration Manager 2012 media.
2. To run the Prerequisite Checker tool, click on the Assess Server Readiness link in the Tools and Standalone Components section.

**NOTE**
The Prerequisite Checker tool has been much enhanced in SCCM 2012. It runs a wider range of checks and is a standalone executable (prereqchk.exe) that can be run unattended via a command line or script. This allows the prerequisite checking process to be automated for large organizations.

3. Remediate any issues the Prerequisite Checker tool finds and click OK to close the window.
4. After ensuring all the prerequisites have been met, click the Install link in the splash screen.
5. At the Before You Begin screen, click Next.
6. Select the Install Configuration Manager Central Administration Site option and click Next.
7. Enter a 25-character product key and click Next.
8. Accept the license terms and click Next.
9. Accept the license terms for the software that will be downloaded and installed automatically on Site Systems pushed through the hierarchy and click Next.

**NOTE**
This automates the prerequisite installations of Microsoft SQL Server 2008 R2 and Microsoft Silverlight for secondary site servers in SCCM 2012. This reduces the amount of preparation needed on a secondary site server and eases the administrative burden of deploying additional servers in the hierarchy.

10. Enter the location to download prerequisites and updates, in this example the previously created share \CM1\SCCMUpdates, and click Next.
11. In the Server Language Selection, leave the default English and click Next.
12. In the Client Language Selection, leave the default English and click Next.
13. In the Site and Installation Settings, enter a site code and site name. In this example, the site code is XYZ and the site name is Company XYZ Central Administration Site.

14. Leave the default installation folder and click Next.

15. In the Database Information, specify the database server name and instance. Click Next.

16. In the SMS Provider Settings, leave the default of CM1 and click Next.

17. In the Customer Experience Improvement Program Configuration, choose the appropriate option and click Next.

18. In the Settings Summary (shown in Figure 3.4), review the settings and click Next.

![Figure 3.4](image)

FIGURE 3.4 The central site installation Settings Summary.

19. The Prerequisite Checker executes a last-minute check. Verify that all prerequisites have been met or remediate any errors, and then click Begin Install.

20. The installation completes and should have green status symbols next to each component installation.

21. Click Close to exit the setup wizard.

Installation is now complete for the Central Administration Site and the console can be launched.
Validating the Installation of the Central Administration Site

To validate the installation, check the contents of the System Management container in Active Directory. The System Management container can be seen by launching Active Directory Users and Computers, selecting the View menu, choosing Advanced Features, and expanding the System folders or with ADSI Edit. The Site Server object should exist in this container for the Central Administration Site. In this example, the XYZ Central Administration Site should create an object in the System Management container named SMS-Site-XYZ of type mSSMSSite. As additional Site Servers in Site System roles are deployed, additional objects are created automatically.

It is important to validate the installation after each role is deployed; this ensures everything is functioning correctly before moving to the next step. It is also important to monitor site status on a continuous basis to ensure the health of the environment. For additional information on automatically monitoring the Configuration Manager hierarchy with Operations Manager, review Chapter 8, “Using Operations Manager 2012 for Monitoring and Alerting.”

In addition, open the Configuration Manager console and review the Site Status component in the System Status container. This console is called Configuration Manager console and is located under the Microsoft System Center 2012\Configuration Manager folder in the Start menu on the Site Server.

To view the Component Status in the ConfigMgr console, do the following:

1. Launch the Configuration Manager console.
2. Choose the Monitoring space.
3. Expand the System Status node.
4. Select the Site Status node and confirm that all statuses show as OK with green icons.
5. Select Component Status and confirm that all statuses show as OK with green icons.

The Site Status page shows a high-level summary of the Site System roles and the status. This is useful for seeing an overview of the Site Systems and ensuring that they are healthy. If a role is marked with a red error or a yellow warning icon, the component has received status messages indicating a problem with the component. Right-click the component, select Show Messages - All from the menu and select a viewing period for the messages.

The Component Status page shows all of the components that make up the Configuration Manager infrastructure for this site. The component status is based on status messages that are received from the component. Because the component has to send the Site Server status, and the Site Server has to process the status message, the condition of components can be delayed. This is especially true when looking at the status of child sites within the Central Site console because status messages are sent to parent sites based on the Site Sender configuration.
If a component is marked with a red error or a yellow warning icon, the component has received status messages indicating a problem with the component. Right-click the component, select Show Messages - All from the menu and select a viewing period for the messages.

**TIP**

The status summarizer for the different components is not automatically changed from red or yellow to green if the component that experienced the problem is fixed. The component summarizer simply counts the number of warning and error status messages that have been received.

To reset the status of a component, right-click the component and select Reset Counts - All from the menu. The count of status messages is reset and the icon will change back to green in a few minutes.

The delay in status messages is often a source of frustration for administrators starting out with Configuration Manager. For a better, real-time view into site components, check the log files with cmtrace.exe, a Configuration Manager 2012 utility. You can identify the log file for a specific component by right-clicking the component and selecting Start, ConfigMgr Service Manager from the menu. Navigate to the component within the Service Manager, right-click the component from the Actions pane, and then select Logging.

**NOTE**

The cmtrace.exe log viewing utility replaces the previous trace32.exe utility from the Configuration Manager toolkit. The cmtrace.exe is included with the SCCM 2012 server and installs with the default setup.

The site component Logging option is shown in Figure 3.5. The SMS Executive logging option has been chosen and shows the name and location of the log file, which is c:\Program Files\Microsoft Configuration Manager\Logs\smsexec.log. The size of the log file, 2 MB, is also shown and can even be adjusted here.

![Configuration Manager Component Logging - Single Component](image.png)

**FIGURE 3.5** The component log location.
Now that the top-level Central Administration Site has been deployed successfully, the primary sites and other sites can be deployed in the Configuration Manager 2012 hierarchy.

**Deploying the Primary Sites**

Deploying primary sites follows a similar process as deploying the Central Administration Site Server. In the case of the Company XYZ Configuration Manager 2012 hierarchy, there are two primary sites. These are San Francisco (SFO) with the CM2 server and Paris (PAR) with the CM3 server.

Verify that all the hardware and software requirements have been met and the installation configuration prerequisites have been completed.

**Installing a Primary Site Server**

Before running the Configuration Manager setup, run the prerequisite checker to verify the required components have been successfully installed. The prerequisite checker can be launched from a link on the splash.hta page. The splash.hta page can be found in the root of the Configuration Manager media.

**TIP**

Make sure the Configuration Manager Site Server Computer Account is in the local administrators group on all component servers and other Site Servers; this includes the Site Database server. The computer account of the Site Server is used to access and manage the remote server by default. One way to accomplish this is by creating a group named **SCCM Site Servers** with the computer accounts of all SCCM Site Servers, then adding the local administrator groups on all Site Servers.

To install the SFO Primary Site Server on the CM2 server in the Company XYZ hierarchy, complete the following steps:

1. Launch splash.hta from the Configuration Manager 2012 media.

2. To run the Prerequisite Checker, click on the Assess Server Readiness link in the Tools and Standalone Components section.

3. Remediate any issues the prerequisite checker tool finds and click OK to close the window.

**NOTE**

It is normal to get a WSUS SDK on site server issue during the prerequisite check on a new Primary Site Server. If this server is intended to host the Site Server Software Update role, then the Windows WSUS role will be installed at that time.
4. After ensuring all the prerequisites have been met, click the Install link in the splash screen.

5. At the Before You Begin screen, click Next.

6. Select the Install Configuration Manager Primary Site option and click Next.

7. Enter a 25-character product key and click Next.

8. Accept the license terms and click Next.

9. Accept the license terms for the software that will be downloaded and installed automatically on Site Systems pushed through the hierarchy and click Next.

**NOTE**

This automates the prerequisites installations of Microsoft SQL Server 2008 R2 and Microsoft Silverlight for secondary site servers in SCCM 2012. This reduces the amount of preparation needed on a secondary site server and eases the administrative burden of deploying additional servers in the hierarchy.

10. Because the prerequisites were downloaded previously, choose the Use Previously Downloaded Files option and enter the location of the downloaded prerequisites and updates, in this example the previously created share `\\CM1\SCCMUpdates`, and click Next.

11. In the Server Language Selection, leave the default English and click Next.

12. In the Client Language Selection, leave the default English and click Next.

13. In the Site and Installation Settings, enter a site code and site name. In this example, the site code is `SFO` and the site name is `Company XYZ San Francisco Site`.

14. Leave the default installation folder and click Next.

15. Enter the name of the Central Administration Site Server to join the existing hierarchy, in this case `cm1.companynxyz.com` and click Next.

16. In the Database Information, specify the database server name and instance. Click Next.

17. In the SMS Provider Settings, leave the default of CM2 and click Next.

18. In the Client Computer Communication Settings, choose the Configure the Communication Method on Each Site System Role option and click Next.

19. In the Site Systems Roles, leave the options to install a Management Point and a Distribution Point checked and click Next.

20. In the Customer Experience Improvement Program Configuration, choose the appropriate option and click Next.
21. In the Settings Summary (shown in Figure 3.6), review the settings and click Next to begin the installation.

![Microsoft System Center 2012 Configuration Manager Setup Wizard](image)

**FIGURE 3.6** The primary Site installation Settings Summary.

22. The Prerequisite Checker executes to do a last-minute check. Verify that all prerequisites have been met or remediate any errors, and then click Begin Install.

23. Installation completes and should have green status symbols next to each component installation.

24. Click Close to exit the setup wizard.

Installation is now complete for the Primary Site and the console can be launched.

Repeat the preceding steps for Company XYZ Paris Site, the PAR Primary Site Server on the CM3 server.

**Validating the Installation of the Primary Site**

To validate the installation, check the contents of the System Management container in Active Directory. The System Management container can be seen with the Advanced view of Active Directory Users and Computers, or with ADSI Edit. In this example, the Site Server object should exist in this container for the Central Administration Site of type `mSSMSSite`. The SFO primary site should create a record in the System Management container named `SMS-Site-SFO` of type `mSSMSSite`. There should also be an object for the Management Point, named `SMS-MP-SFO-CM2.COMPANYXYZ.COM` of type `mSSMSManagementPoint`. Similarly, the PAR primary site should create an object in the
System Management container named SMS-Site-PAR of type mSSMSSite. There should also be an object for the Management Point, named SMS-MP-PAR-CM3.COMPANYXYZ.COM of type mSSMSManagementPoint. Figure 3.7 shows the Active Directory records for the sites created.

![Active Directory SCCM records for Primary Sites.](image)

**FIGURE 3.7** The Active Directory SCCM records for Primary Sites.

It is important to validate the installation after each role is deployed; this ensures everything is functioning correctly before moving to the next step. It is also important to monitor site status on a continuous basis to ensure the health of the environment. For additional information on automatically monitoring the Configuration Manager hierarchy with Operations Manager, review Chapter 8.

In addition, open the Configuration Manager console located under the Microsoft System Center 2012\Configuration Manager folder in the Start menu on the Site Server, expand the Monitoring option, and review the Site Status component in the System Status container.

To view the component status in the Configuration Manager console, do the following:

1. Launch the Configuration Manager console.
2. Choose the Monitoring space.
3. Expand the System Status node.
4. Select the Site Status node and confirm that all statuses show as OK with green icons.
5. Select Component Status and confirm that all statuses show as OK with green icons.
The Site Status page shows a high-level summary of the Site System roles and the status. This is useful for seeing an overview of the Site Systems and ensuring that they are healthy. If a role is marked with a red error or a yellow warning icon, the component has received status messages indicating a problem with the component. Right-click the component, select Show Messages - All from the menu and select a viewing period for the messages.

The Component Status page shows all of the components that make up the Configuration Manager infrastructure for this site. The component status is based on status messages that are received from the component. Because the component has to send the Site Server status, and the Site Server has to process the status message, the condition of components can be delayed. This is especially true when looking at the status of child sites within the Central Site console because status messages are sent to parent sites based on the Site Sender configuration.

If a component is marked with a red error or a yellow warning icon, the component has received status messages indicating a problem with the component. Right-click the component, select Show Messages - All from the menu, and select a viewing period for the messages.

**TIP**

The status summarizer for the different components is not automatically changed from red or yellow to green if the component that experienced the problem is fixed. The component summarizer simply counts the number of warning and error status messages that have been received.

To reset the status of a component, right-click the component and select Reset Counts - All from the menu. The count of status messages is reset and the icon will change back to green in a few minutes.

The delay in status messages is often a source of frustration for administrators starting out with Configuration Manager. For a better, real-time view into site components, check the log files with `cmtrace.exe`, a Configuration Manager 2012 utility. You can identify the log file for a specific component by right-clicking the component and selecting Start, ConfigMgr Service Manager from the menu. Navigate to the component within the Service Manager, right-click the component from the Actions pane, and then select Logging.

**NOTE**

The `cmtrace.exe` log viewing utility replaces the previous `trace32.exe` utility from the Configuration Manager toolkit. The `cmtrace.exe` is included with the SCCM 2012 server and installs with the default setup.

Now that the primary sites have been deployed successfully, the secondary sites can be deployed in the Configuration Manager 2012 hierarchy.
Deploying the Secondary Sites

Configuration Manager 2012 secondary sites are deployed through the console, via a push from a Primary Site Server. All the prerequisites, such as SQL Server 2008 and .NET Framework 4.0, are pushed out with the role remotely. However, this requires two features to be installed to work correctly. Those features are as follows:

- Remote Differential Compression
- .NET Framework 3.5

To install these prerequisites using the command line, run PowerShell as an administrator and enter the following commands:

```powershell
Import-Module ServerManager
Add-WindowsFeature Net-Framework,RDC
```

In addition, the Primary Site Server Active Directory account (for example, CM3$) is the account performing the remote installation, so it must have local administrator rights to the target secondary site server.

If the Windows Firewall is in use, open ports 1433 and 4022 for SQL Server access.

**TIP**

The computer account of the Site Server is used to access and manage the remote secondary site server by default. One way to accomplish this is by creating a group named SCCM Site Servers with the computer accounts of all SCCM Site Servers, then adding the local administrator groups on all Site Servers.

To deploy a secondary site from a primary site, execute the following steps:

1. Launch the Configuration Manager console.

**NOTE**

The Configuration Manager console can be launched from the Central Administration Site Server or the Primary Site Server. Even if the installation is initiated with the Configuration Manager console on the Central Administration Site, the actual installation is performed from the Primary Site Server. This is a great example of the improved centralized administration capabilities of Configuration Manager 2012.

2. Choose the Administration space, expand Site Configuration, and select Sites.

3. Select the primary site from which to deploy the secondary site, in this example the PAR site.

4. Right-click on the Primary Site Server (the CM3 server in this example) and select Create Secondary Site.
5. At the Before You Begin screen, click Next.

6. In the Site and Installation Settings, enter a site code, Site Server, and site name. In this example, the site code is LON, the server is cm4.companyxyz.com, and the site name is Company XYZ London Site.

**NOTE**
The case of the server name is critical, as the install will fail if the name in the fully qualified domain name (FQDN) does not match the NetBIOS name exactly. If this happens, simply right-click on the failed installation and select Retry Secondary Site and change the case of the server name.

7. Leave the default installation folder and click Next.

8. Leave the default to copy the installation source files from the parent Site Server (in this case cm3.companyxyz.com) and click Next.

9. Leave the default to install SQL Server Express on the secondary site server and click Next.

10. Make sure to check the Install and Configure IIS option, as shown in Figure 3.8, and click Next.

![FIGURE 3.8 Specify Distribution Point Settings.](image-url)
NOTE
Later in the chapter, when configuring Internet-based client management (IBCM), the protocol setting will be changed from HTTP to HTTPS.

11. Leave the default drive settings and click Next.

12. Leave the default Content Validation settings and click Next.

13. Leave the Boundary Groups settings empty and click Next. These will be configured later.

14. Review the summary and click Next.

15. Click Close to exit the wizard.

The setup begins from the Primary Site Server. A new Site Server appears in the list of sites with a status of Pending. To see the summary status, right-click on the secondary server and select Show Install Status. This shows the summary status message for the secondary site server install.

Because installation is being done remotely, it can be difficult to ascertain what could’ve gone wrong with the installation. However, the Show Install Status messages are very informative and specific. They show the prerequisite checks being done, the download progress, and the installation progress step-by-step. In the event of a failure of the secondary site installation, these messages can be reviewed for the specific reason for the failure. Once remediated, the secondary site server installation can be retried simply by right-clicking the failed secondary site server and selecting Retry Secondary Site.

TIP
The status of the secondary site server install can also be monitored in detail from the source Primary Site Server and the target secondary site server. In the root of the system drive of the Primary Site Server doing the push installation, the log file ConfigMgrSetup.log will show the status of the install in detail. Once the installation commences, there will be a corresponding ConfigMgrSetup.log in the root of the system drive of the secondary site server, which shows where the installation picks up locally. Review the log on the source Primary Site Server to troubleshoot remote access and file transfer issues. Review the log on the target secondary site server to troubleshoot issues with the installation of prerequisites and the secondary site role.

Validating the Installation of the Secondary Site
To validate the installation, check the contents of the System Management container in Active Directory. The System Management container can be seen with the Advanced view of Active Directory Users and Computers, or with ADSI Edit. The Site Server object should exist in this container for the Secondary Sites. In this example, the LON secondary site should create an object in the System Management container named SMS-Site-LON of
type mSSMSSite. There should also be an object for the Management Point, named SMS-MP-LON-CM4.COMPANYXYZ.COM of type mSSMSSManagementPoint. Similarly, the TOK secondary site should create an object in the System Management container named SMS-Site-TOK of type mSSMSSite. There should also be an object for the Management Point, named SMS-MP-TOK-CM5.COMPANYXYZ.COM of type mSSMSSManagementPoint. Figure 3.9 shows the Active Directory objects for the sites created.

![Image](image.png)

**FIGURE 3.9** The Active Directory SCCM records for Secondary Sites.

To view the component status for the secondary site servers in the Configuration Manager console, do the following:

1. Launch the Configuration Manager console.
2. Choose the Monitoring space.
3. Expand the System Status node.
4. Select the Site Status node and confirm that all statuses show as OK with green icons.
5. Select Component Status and confirm that all statuses show as OK with green icons.

If a component is marked with a red error or a yellow warning icon, the component has received status messages indicating a problem with the component. Right-click the component, select Show Messages - All from the menu and select a viewing period for the messages.
TIP

Sometime, the secondary site server installation process will not correctly install
the prerequisite Background Intelligent Transfer Service (BITS) Windows feature.
If this is the case, there’ll be Message ID 4957 error messages in the
SMS_MP_CONTROL_MANAGER component for the secondary site server. Add the BITS
feature manually on the secondary site server if this occurs. The errors should resolve
themselves in the next hourly cycle.

Configuring the Hierarchy

With the SCCM 2012 servers deployed, the next task is to configure the hierarchy.
Configuration Manager 2012 deploys a more complete set of roles by default than the
previous versions, but there still remain roles to be configured. The Configuration
Manager 2012 console is divided into four spaces: Assets and Compliance, Software
Library, Monitoring, and Administration. The hierarchy configuration takes place within
the Administration space.

The Site Settings container within the Site Management node can be used to configure
the different components and functionality provided by Configuration Manager. Prior to
managing clients, the appropriate functionality should be implemented and configured to
ensure clients are managed properly following the agent deployment.

The Configuration Manager console with the Administration space expanded is shown in
Figure 3.10. This view also has the sites selected and shows the five servers that have been
deployed (CM1, CM2, CM3, CM4, and CM5) in the Company XYZ infrastructure.

FIGURE 3.10 The Configuration Manager console Administration space.
Establishing Boundaries and Boundary Groups

Establishing site boundaries and boundary groups is one of the most important aspects of Configuration Manager. Boundaries let managed systems receive content and communicate status to the closest server in the Configuration Manager hierarchy.

The boundaries, in effect, map physical locations, based on IP address, to systems such as workstations. Boundary groups allow administrators to logically group boundaries together and then assign resources such as Distribution Points for them to use.

Boundaries can be created based on IP subnet, IPv6 prefix, IP address range, and Active Directory sites. Typically in an Active Directory environment, the Configuration Manager is based on Active Directory site boundaries. Because the Active Directory site infrastructure should already map directly to the network topology, many of the same principles that apply to an Active Directory site topology also apply to the Configuration Manager topology. For example, instead of taking all the subnets in a specific network location and adding them as a site boundary, it is much easier to add the already configured Active Directory site boundary.

That said, there are still many different scenarios and environments where using an Active Directory site boundary simply isn’t possible or practical for technical or even political justification. Configuration Manager allows a mixture of all the different boundaries. It is possible to configure different combinations of site boundaries in the console to address these scenarios.

**CAUTION**

Never configure overlapping boundaries. This can cause managed systems to use the wrong Site Server or Distribution Management Point. This often happens when using a combination of IP and Active Directory boundaries.

New to Configuration Manager 2012 is the ability to have the Active Directory sites be discovered automatically in the forest. This saves a tremendous amount of time. The Active Directory forest discovery operates very similarly to the Active Directory system discovery or group discovery.

To configure Active Directory forest discovery, do the following:

**NOTE**

Launching the console on the Central Administration Site provides complete administrative access to the entire Configuration Manager 2012 hierarchy.

1. Launch the Configuration Manager console on the Central Administration Server.
2. Choose the Administration space.
3. Expand the Hierarchy Configuration and select Discovery Methods.
4. Right-click on Active Directory Forest Discovery and select Properties.

5. Check Enable Active Directory Forest Discovery and the check box to automatically create site boundaries.

6. Change the Schedule option to run every day.

7. Click OK to save changes and Yes to run the full discoveries as possible.

Once the Active Directory forest discovery is completed, the Active Directory site boundaries will be created. Figure 3.11 shows the Active Directory site boundaries created for the Company XYZ organization.

Boundary groups are not discovered automatically, but rather are configured by the administrator. Boundary groups logically group the agents (through the boundaries) with resources such as Management Points and Distribution Points. This allows administrators to control where agents download their content from, thus controlling bandwidth utilization. For example, the Company XYZ organization has five locations: San Francisco, Paris, London, Tokyo, and New York. New York is the only office without a Configuration Manager 2012 Site Server. Boundary groups will be created for each location with the Site Server, so that local clients will download content from the local Site Servers. However, the New York boundary will be added to the SFO boundary group to ensure that the New York agents download content from the San Francisco Site Server. These boundary groups are shown in Figure 3.12.
To create a boundary group (in this example the Company XYZ SFO boundary group), execute the following steps:

1. Make sure that your Active Directory sites and subnets are configured correctly and include all subnets and physical sites in the environment.

2. Launch the Configuration Manager console on the Central Administration Site Server.

3. Choose the Administration space.

4. Expand the Hierarchy Configuration and select the Boundary Groups node.

5. Right-click on the boundary group node and select Create Boundary Group.

6. In the general tab, enter the name of the boundary group (in this case, **SFO**).

7. Click the Add button to add boundaries to the boundary group.

8. Check the SFO boundary, and then click OK.

9. Choose the Reference tab.

10. In the Site Assignment section, check the Use This Boundary Group for Site Assignment check box and select the SFO site in the drop-down.

11. In the Content Location section, click the Add button.

12. Select the SFO Site Server and click OK.
NOTE

The connection defaults to “Fast.” This can be changed to “Slow” by clicking on the Change Connection button. This can be used to control how content is downloaded or if content is downloaded. This is useful for having backup content locations.

13. Click OK to create the boundary group.

When a server is configured within a boundary group, the server connection type defaults to Fast. The connection types are limited to Fast or Slow and are somewhat misleading. The true purpose of the connection types is during the creation of a deployment. When you want to deploy software, such as an application or patches, to a system, a deployment is needed. When configuring the deployment, several different distribution options are available. The deployment distribution options are shown in Figure 3.13.

![Figure 3.13 Distribution options.](image)

The deployment allows the administrator to specify distribution characteristics depending on the configuration of the boundary groups. For example, if you configure a server connection in the boundary group as Slow and then configure the deployment to not run when the client is connected to a slow or unreliable network boundary, the software will not run on any system that identifies itself as being within this boundary.

NOTE

The topic of deployments is covered in Chapter 4 “Using Configuration Manager 2012 to Distribute Applications, Updates, and Operating Systems.”
The remaining boundary groups for Paris, London, and Tokyo can be created following the previous procedure. Now clients in the boundaries will automatically assign themselves to the appropriate site and download content from the appropriate location.

### Configuring Discovery Methods

The Active Directory System Discovery option is the most common method used to find potential systems to manage. The main advantage to the AD System Discovery option is its efficiency in a well-maintained domain. Ensure that computer accounts that are no longer used have been disabled or removed from the Active Directory domain.

**NOTE**

Discovery of systems, groups, and users can be configured on each primary site in the SCCM 2012 hierarchy. However, discovery information is shared with all sites in the hierarchy. Rather than have duplicate discoveries, the best practice is to designate a single primary site in the hierarchy to do the discovery.

To enable the Active Directory System Discovery method, do the following:

1. From the ConfigMgr console, select the Administration space and expand the Hierarchy Configuration folder.
2. Select the Discovery Methods node.
3. Right-click and open the properties of the Active Directory System Discovery method for the SFO site. The SFO site will be the Company XYZ designated discovery site.
4. Enable Active Directory System Discovery.
5. Click the “*” button to add an AD container.
6. Click the Browse button and then click OK to select the entire companyxyz.com domain.
7. Accept the default options and click OK.
8. Select the Polling Schedule tab and click the Schedule button.
9. Change the recurrence to 1 hour and click OK.
10. Click OK to save the changes.
11. Click Yes at the pop-up to run the full discovery as soon as possible.

The status of the AD system discovery can be viewed in the adsysdis.log file.

To review the results of the discovery, do the following:

1. From the ConfigMgr console, expand Asset and Compliance.
2. Expand Overview, expand Devices, and right-click on the All Systems collection.
3. Click Update Membership.
4. Click Yes when prompted.
5. Click the Refresh action.

The collection should show all of the clients in the domain.

To enable the Active Directory Group Discovery method, do the following:

1. From the ConfigMgr console, select the Administration space and expand the Hierarchy Configuration folder.
2. Select the Discovery Methods node.
3. Open the properties of the Active Directory Group Discovery method for the SFO site. The SFO site will be the Company XYZ designated discovery site.
4. Enable Active Directory Group Discovery.
5. Click the Add button and select a location. Enter **Company XYZ Domain** for the Name.

**NOTE**

Active Directory Group Discovery supports the discovery of single groups for all groups with the location, such as a domain.

6. Click the Browse button and then click OK to select the entire companyxyz.com domain.
7. Accept the default options and click OK.
8. Select the Polling Schedule tab and click the Schedule button.
9. Change the recurrence to 1 hour and click OK.
10. Click OK to save the changes.
11. Click Yes at the pop-up to run the full discovery as soon as possible.

The previous steps should be repeated for the Active Directory User Discovery for SFO.

The Active Directory discoveries can be triggered manually by right-clicking on the discovery method and selecting Run Full Discovery Now. The detailed results of the discovery can be seen in the log files on the discovery server. The log files for each of the discoveries are as follows:

- Active Directory System Discovery (*adsysdis.log*)
- Active Directory Group Discovery (*adsgdis.log*)
- Active Directory User Discovery (*adusrdis.log*)

Any discovery errors or access errors will be shown in these detailed logs.
Configuring Hierarchy and Geographic Views

Configuration Manager infrastructures can be complex and hard to monitor. A very common request for administrators is to be able to view the hierarchy in a dynamic way. Another very common request is for administrators to be able to see their hierarchy map out geographically, with components in the correct place on a map. Configuration Manager 2012 delivers on both these requests.

The Configuration Manager 2012 hierarchy diagram shows the hierarchy in a graphical, dynamic, and active view. Each site is displayed in the diagram, with links and status. As sites are added and states change, the hierarchy diagram will update automatically.

Figure 3.14 shows the hierarchy diagram for Company XYZ. The diagram shows each of the five Configuration Manager 2012 Site Servers with a different icon for each site type. The overall alert status for each site is indicated as well, as can be seen in the warning state for the PAR site. Right-clicking on any component gives you detailed status, as is shown for the SFO site. The detailed status also allows you to link to key information such as site status messages and site properties.

To access the hierarchy diagram, do the following:

1. Launch the Configuration Manager console.
2. Select the Administration space.
3. Select the Site Hierarchy folder.
In addition to the hierarchy diagram, there is also a geographical view. This view shows all the Site Servers on a Bing map. However, physical location information needs to be specified to enable the display of Site Servers on the map.

To specify the location information and display the geographical view, execute the following steps:

1. Launch the Configuration Manager console.
2. Select the Monitoring space.
3. Select the Site Hierarchy folder.
4. Right-click the Site Hierarchy folder and select Configure View Settings.
5. Select the Site Location tab.
6. For each site, enter a location. The location can be general, such as the city, or specific, such as the address.
7. Click OK to save the changes.
8. Right-click the Site Hierarchy folder and select Geographical View.

The view now shows a world map with the Site Servers correctly placed in their locations, as shown in Figure 3.15.

![Company XYZ geographical view](image)

**FIGURE 3.15** Company XYZ geographical view.
Like the hierarchy view, when the geographical view is active, hovering over a site with a mouse gives a high-level alert status and subsite count. The basis for the underlying map is the Bing Map engine. The map can be viewed either as a road map or an aerial satellite view. The map can also be zoomed into, to get detailed street information. In addition, selecting a site shows site links to neighboring sites. Figure 3.16 shows a zoom into the Company XYZ European region, with expanded map detail. The Paris site has been selected, which then shows the site links, including the site link to London.

NOTE
If it displays some instructions instead of the Bing Map, it may be because of the server’s Internet Explorer settings; follow the instructions to solve the issue.

Either view can be printed to capture the key information. The hierarchy diagram and the geographical view provide exciting new and dynamic ways to view the Configuration Manager 2012 infrastructure.

Configuring Exchange Connectors
The Configuration Manager 2012 Exchange connector allows administrators to manage mobile devices that do not or cannot have agents installed on them, such as Apple iPhone, Apple iPad, or Google Android devices. Essentially any device that supports ActiveSync and is connected to Exchange Server can be managed through the connector.
To configure the Exchange connector, do the following steps:

1. Launch the Configuration Manager console.
2. Choose the Administration space.
3. Expand the Hierarchy Configuration folder.
4. Right-click on the Exchange Server Connectors node and select Add Exchange Server.
5. In the Server Address (URL) field, enter the address of the Exchange Client Access Server. The format of the URL is http://excas.companyxyz.com/powershell.
6. Select the Configuration Manager site to run the Exchange Server connector.
7. Click Next.
8. In the Account section, enter the account with which to connect to the Exchange server and click Next.

**NOTE**
The Account page very helpfully lists the Exchange Server cmdlets that the connector will need to be able to run the function correctly. The specified account should have the appropriate rights to run those cmdlets.

9. In the Discovery page, leave the defaults and click Next.
10. Adjust the policy settings as needed, and then click Next.
11. Review the summary and click Next to create the connector.

The connector will automatically synchronize with the targeted Exchange server. The synchronization can be forced by right-clicking on the connector and selecting Synchronize Now. Mobile devices will appear shortly in the list of devices.

**Configuring Sites**

Configuration Manager 2012 deploys certain Site System roles such as Management Points and Distribution Points, but does not deploy other roles nor completely configure those that it does deploy by default. Site configuration entails completing the configuration of the deployed roles and deploying of the required roles.

When deploying Site System roles to either the Site Server or a remote server, it is important to note the component installation wizard doesn’t actually do the installation—it simply queues the installation for the Site Component Manager service. Even through the wizard always completes with a successful message, it is important to review the corresponding log files and the System Status container to ensure the component was actually installed correctly.
The log files for component installation are typically located on the server the component is being installed on, in a folder called \Program Files\Microsoft Configuration Manager\Logs. Additional status messages can be viewed in the sitecomp.log file on the Primary Site Server.

**Deploying the Fallback Status Point Role**

The Fallback Status Point (FSP) is very important. It provides a safety net for clients. The Configuration Manager agent should always be able to communicate status messages to the FSP, even if other communication has failed or is being blocked due to certificate or other issues.

To install FSP, complete the following steps:

1. From within the Administration space, expand Site Configuration and select Servers and Site Systems Roles.
2. Right-click CM2 and select Add Site System Roles.
3. On the General page, click Next.
4. Enable the Fallback Status Point role and click Next.
5. Accept the default configuration and click Next.

**TIP**

When a client is deployed, it sends several status messages to the FSP, even when the deployment is successful. If a large client rollout is planned, increase the number of messages allowed to prevent a backlog.

6. Review the summary and click Next.
7. Wait for the installation to complete, and then close the wizard.

Review the fspMSI.log and the SMFSFSPSetup.log files for installation status. During normal operation, problems can be identified with the fspmgr.log file and using reports such as the Client Deployment Status Details or the Client Deployment Failure report.

**Deploying the Reporting Service Point Role**

The Reporting Service Point (RSP) provides reporting of Configuration Manager data through SQL Reporting Services (SRS). SRS is a significantly more powerful platform for developing and delivering reports.

The Reporting Service Point component is installed in three steps. Initially, the role is added to the correct server from the Site Management\Site Systems node. Then the Reporting Point needs to be configured with a data source; this is necessary to establish communication with the database holding the Configuration Manager data. Finally, reports need to be migrated from the legacy Reporting Point to the Reporting Service Point.
To install RSP on the Central Administration Site (CM1), complete the following steps:

1. From within the Administration space, select Servers and the Site System Roles folder.
2. Right-click CM1 and select Add Site System Roles.
3. On the General page, click Next.
4. Enable the Reporting Services Point role and click Next.
5. The Site Database Connection Settings will be discovered automatically. Click the Verify button to verify the settings.
6. In the Reporting Services Point Account, click the Set button and choose New Account.
7. Enter the appropriate credentials, and then click OK.
8. Click Next.
9. Review the summary and click Next.
10. Wait for the installation to complete, and then close the wizard.

This process should be completed not only for the Central Administration Site, but also for each primary site as well. This allows each of the sites to generate reports covering their specific information. For example, reports generated from the Central Administration Site in San Francisco will include information from the entire Company XYZ hierarchy. Reports generated from either the SFO or PAR primary sites will only include information from their portion of the hierarchy.

Review the SRSRPSsetup.1og and the srsrp.1og files. These log files are located on the server hosting the Reporting Service Point in the Configuration Manager log folder (often c:\Program Files\Microsoft Configuration Manager\Logs). To check the status of the Reporting Services Point, go to the Monitoring space in the console, expand the Reporting folder, and select the Reports node. Reports will be listed there once the role is completed deploying.

**Deploying Software Updates Point Role**

For Site Servers that will be supporting the Software Updates role, there are two parts to the role setup. The first is to set up Windows Server Update Services (WSUS) and the second is to set up the Software Update Point role. In a Configuration Manager 2012 hierarchy that includes a Central Administration Site, the Software Update Point role will be installed on the Central Administration Site Server.

The Windows Server Update Services (WSUS) 3.0 SP2 components are required by Configuration Manager to support synchronization of patch data from Microsoft Update. WSUS is not used to deliver patches to managed systems; instead, the Configuration Manager hierarchy is used to effectively create an enterprise patch delivery and installation system.
To install WSUS 3.0 SP2, do the following on the Central Site Server (CM1 in the Company XYZ hierarchy):

1. Launch Windows Server Manager.
2. Right-click on the Roles folder and select Add Roles.
3. Click Next to skip the Welcome page.
4. Check the Windows Server Update Services role.
5. Click the Add Required Role Services if it pops up.
6. Click Next.
7. Click Next and Next past the Web Server (IIS) options.
8. At the WSUS welcome screen, click Next.
9. At the Confirmation screen, click Install.

**NOTE**
The WSUS installer downloads the latest version from the Internet and launches, continuing the installation.

10. Once the Windows Server Update Services 3.0 SP2 Setup Wizard launches, at the Welcome screen click Next.
11. Accept the terms of the license agreement and click Next.
12. Store the updates on c:\WSUS and click Next.
13. Select Using an Existing Database Server on This Computer.
14. Click Next.
15. If the connection is successful, click Next.
16. Leave the default website preference and then click Next.
17. Review the installation configuration and click Next.
18. Close the wizard when the installation is complete.

**NOTE**
There is no need to bother with the WSUS Configuration Wizard. All configuration of WSUS will be administered and managed using the Configuration Manager console.
Once the Windows WSUS role has been installed, the next step is to deploy the Software Update Point role. To do this, complete the following steps:

1. On the Central Administration Site Server (CM1 in the Company XYZ hierarchy), launch the Configuration Manager console.
2. In the Administration space, expand the Site Configuration folder and select the Servers and Site System Roles node.
3. Right-click the Central Administration Site Server, in this case CM1, and choose Add Site System Roles.
4. Click Next.
5. Check the Software Update Point role and click Next.
6. At the Software Update Point screen, leave the defaults and click Next.
7. At the Active Settings screen, check the Use This Server as the Active Software Update Point check box and click Next.
8. At the Synchronization Source screen, leave the defaults and click Next.
9. At the Synchronization Schedule screen, check the Enable Synchronization on a Schedule check box.
10. Change the schedule to run every 1 Days and click Next.
11. At the Supersedence Rules screen, leave the default and click Next.
12. At the Classifications screen, check All Classifications and click Next.
13. At the Products screen, check the required products and click Next.
14. At the Languages screen, check the appropriate languages and click Next.
15. Review the summary screen and then click Next.
16. Close the wizard when completed.

The Central Administration Site will now perform update synchronization for the entire Configuration Manager 2012 hierarchy.

**Deploying Endpoint Protection Point Role**

In Configuration Manager 2012, the System Center 2012 Endpoint Protection is integrated into the product rather than a separate install. There is now a Site Server role called Endpoint Protection Point, which provides endpoint protection services.

In a Configuration Manager 2012 hierarchy that includes a Central Administration Site, the Endpoint Protection Point role will be installed on the Central Administration Site Server.
To deploy the Endpoint Protection Point role, complete the following steps:

1. On the Central Administration Site Server (CM1 in the Company XYZ hierarchy), launch the Configuration Manager console.

2. In the Administration space, expand the Site Configuration folder and select the Servers and Site System Roles node.

3. Right-click the Central Administration Site Server, in this case CM1, and choose Add Site System Roles.

4. Click Next.

5. Check the Endpoint Protection Point role.

6. There will be a pop-up warning that software updates require special configuration or endpoint protection needs to use a different source. Click OK.

7. Click Next.

8. At the Endpoint Protection screen, accept the license terms and click Next.

9. Choose the appropriate Microsoft Active Protections Service (MAPS) membership type and click Next.

10. Review the summary screen and then click Next.

11. Close the wizard when completed.

The Central Administration Site will now perform endpoint protection for the entire Configuration Manager 2012 hierarchy.

**Deploying Asset Intelligence Synchronization Point Role**

An additional component called the Asset Intelligence Synchronization Point is also available. This component provides integration between Configuration Manager and Microsoft System Center Online services provided by Microsoft.

In a Configuration Manager 2012 hierarchy that includes a Central Administration Site, the Asset Intelligence Synchronization Point role will be installed on the Central Administration Site Server.

To deploy the Asset Intelligence Synchronization Point role, follow these steps:

1. On the Central Administration Site Server (CM1 in the Company XYZ hierarchy), launch the Configuration Manager console.

2. In the Administration space, expand the Site Configuration folder and select the Servers and Site System Roles node.

3. Right-click the Central Administration Site Server, in this case CM1, and choose Add Site System Roles.

4. Click Next.
5. Check the Asset Intelligence Synchronization Point role and click Next.

6. At the Asset Intelligence Synchronization Point Settings screen, leave the defaults and click Next.

**NOTE**

A certificate is not required. This was a legacy requirement back when Microsoft controlled what organizations could do asset intelligence synchronization, limiting it to organizations with Software Assurance contracts. After a time, Microsoft relaxed the requirement and now allows all organizations to perform asset intelligence synchronization without the certificate requirement.

7. At the Proxy Server Settings screen, leave the defaults and click Next.

8. At the Synchronization Schedule screen, leave the Enable Synchronization on a Schedule check box checked.

9. Change the schedule to run every one days and click Next.

10. Review the summary screen and then click Next.

11. Close the wizard when completed.

The Central Administration Site will now perform asset intelligence synchronization for the entire Configuration Manager 2012 hierarchy.

**Preparing for OS Deployment**

To support OS deployment user state migration and using network boot, the State Migration Point and PXE-enabled Distribution Point are required. To also support a complete operating system refresh with the ability to capture the users’ existing settings, store them securely on the network, then reapply them to the new operating system; the State Migration Point is required.

The PXE functionality requires the WDS transport feature. This is available by default on Windows Server 2008, and can be installed automatically during the PXE configuration.

To enable CM2 to support PXE for OS deployment, complete the following steps:

1. Launch the Configuration Manager console.

2. In the Administration space, expand the Site Configuration folder and select the Servers and Site System Roles node.

3. Select the Primary Site Server, in this case CM2, and choose the Distribution Point role from the details window below.

4. Right-click the Distribution Point role and select Properties.
5. Select the PXE tab.
6. Enable PXE support for clients.
7. Click Yes after reviewing the ports information pop-up.
8. Check the Allow This Distribution Point to Respond to Incoming PXE Requests check box.
9. Check the Enable Unknown Computer Support check box and click OK to the warning pop-up.
10. Uncheck the Require a Password when Computers Use PXE check box.
11. Click OK to save changes to the Distribution Point.

The next step is to install the State Migration Point. This allows systems that are undergoing operating system deployment to upload the captured user state and then download the captured user state once the operating system is upgraded.

To deploy the State Migration Point role, follow these steps:

1. Launch the Configuration Manager console.
2. In the Administration space, expand the Site Configuration folder and select the Servers and Site System Roles node.
3. Right-click the Primary Site Server, in this case CM2, and choose Add Site System Roles.
4. Click Next.
5. Select the State Migration Point and click Next.
6. Click the orange “*” to specify a new folder to store state.
7. Enter a folder to use, such as `c:\StateMigration` and click OK.
8. Click Next.
9. Leave the default boundary groups and click Next.
10. Review the summary screen and then click Next.
11. Close the wizard when completed.

The preceding steps to configure PXE functionality and state migration functionality need to be completed on each Distribution Point and Site Server where Operating System Deployment (OSD) functionality is needed. Typically, this is all Primary Site Servers and all secondary site servers in the Configuration Manager 2012 hierarchy, as well as locations with just Distribution Points.
Configuring Client Settings

Client settings control 18 different areas of client configuration, ranging from BITS configuration through User and Device Affinity. In the past, these settings were monolithic and applied to the entire site. There was no granularity within the site nor any way to transfer settings across the hierarchy. In Configuration Manager 2012, the client settings are configured at a hierarchy level, meaning that the settings apply to the site and all child sites. In addition, custom settings can be created and deployed to collections. These custom settings and flexible targeting mechanism allow settings to be adjusted in a very fine-grained manner.

In the next sections, each of the settings are covered along with recommended settings. To review and edit any of the settings, select the Administration space.

Background Intelligent Transfer

The Background Intelligent Transfer settings allow administrators to control the download behavior of clients via the BITS protocol. By default, these settings are disabled, but if enabled, these settings allow the client to be throttled within a specified window with maximum transfer rates.

For most organizations, it is recommended that this be left disabled.

Client Policy

The client policy settings control how often the client checks in for policy updates, by default every 60 minutes. This essentially establishes a heartbeat for the policy refresh. If new policies are deployed, this polling interval limits how quickly that policy can be deployed.

This was a classic example where different settings were needed for different types of devices. Many organizations were comfortable with a one-hour polling interval for workstations, but wanted a much shorter polling interval for servers along the lines of 15 minutes. This was difficult to do in previous versions of SCCM, but in SCCM 2012 is easy to do with the custom client settings targeted at servers.

In addition, user policy polling can be disabled or enabled. This controls whether users will see user policy. Machine policies are always applied.

It is recommended that the default polling interval of 60 minutes be left in place unless there are specific reasons to adjust it.

Compliance Settings

The Compliance Settings section controls whether compliance is enabled or disabled. This setting is enabled by default. The schedule for compliance evaluation is also set in this section, with the default of every seven days.

It is recommended that compliance evaluation be left enabled and that schedule be adjusted to run every one day.
Computer Agent
The Computer Agent section contains a smorgasbord of settings related to notifications, the Application Catalog, and installation permissions. A few of these have very useful applications.

The Install Permissions setting allows administrators to control which users can initiate installation of software and software updates in task sequences. The options are as follows:

- All Users
- Only Administrators
- Only Administrators and Primary Users
- No Users

This setting, in combination with custom settings targeted at collections, allows administrators to control who is allowed to manually install software advertised by SCCM.

The PowerShell Execution Policy allows administrators to control whether unsigned PowerShell scripts are allowed or not. The default Restricted setting prevents unsigned scripts from executing, whereas the Bypass setting allows unsigned scripts to execute.

The Deployment Deadline options control how often users will see pop-ups of impending deployment deadlines over 24 hours out, less than 24 hours out, and less than an hour away. This set of options combined with custom settings targeted at collections allows administrators flexibility in notifying users.

Computer Restart
The Computer Restart section controls the notifications that users receive before pending restart. The temporary notification, by default 90 minutes, is the advance warning the user gets before restart. The countdown notification, by default 15 minutes, is the countdown window that the user gets before restart.

Endpoint Protection
The Endpoint Protection section covers the settings related to the Microsoft anti-malware features of Configuration Manager 2012. It is disabled by default, but is highly recommended that it be enabled.

Most of the settings in this section control agent installation behavior, such as to install the agent (default is True), remove previously installed agents (default is True), and suppress restarts after installation (default is True).

Interestingly, the default remove previously installed agents will remove both Microsoft and non-Microsoft antivirus agents. The list of antivirus agents that will be removed includes the following:
• All current Microsoft anti-malware products except for Windows InTune and Microsoft Security Essentials
• Symantec AntiVirus Corporate Edition version 10
• Symantec Endpoint Protection version 11
• Symantec Endpoint Protection Small Business Edition version 12
• Mcafee VirusScan Enterprise version 8
• Trend Micro OfficeScan

Given the ease with which SCCM 2012 endpoint protection deploys, it may come as a surprise when it uninstalls other antivirus agents. To prevent this, it is recommended to use custom client settings with this option disabled.

The one setting that needs to be changed, after enabling the agent, is the Disable Alternate Sources option. This is enabled by default, which prevents the Endpoint Protection agent from using other sources such as Microsoft Windows Update to get definition updates. This option should be set to False, to allow the agent to get definition updates from Windows Update.

**Hardware Inventory**

The Hardware Inventory section, enabled by default, primarily controls the interval on which hardware inventory is collected. The default of seven days is usually too long and it is recommended to change the schedule to once per day.

In addition, in this section additional hardware inventory classes can be configured to be collected. This includes Registry values for other important information, which previously required modifying text files directly. Embedding a graphical user interface (GUI) to do this in Configuration Manager 2012 is a very welcome enhancement.

**Remote Tools**

The Remote Tools section controls the remote tools if enabled on agents and the behavior of the remote tools if it is enabled. Remote tools are by default disabled.

A new feature of the remote tools settings is the ability to set the Windows Firewall as part of enabling the tool. As shown in Figure 3.17, the remote control feature is enabled in the check box to configure the remote control port and program exception for just the domain firewall. This ensures that while computers are connected to the domain, remote control will be allowed through the firewall. When not connected to the domain, those ports will be closed and not present a security risk.
Another welcome enhancement to Configuration Manager 2012 is the Allow Remote Control of an Unattended Computer option. This feature was completely absent from the previous version of SCCM, meaning that the user always had to be present when using remote tools. With SCCM 2012, administrators can now press Ctrl+Alt+Delete on a remote agent. However, this is explicitly allowed (the default) or disallowed in the remote tools client settings.

**Software Deployment**

In the Software Deployment section, the only setting is for the deployment reevaluation schedule. This defaults to seven days and can be left at the default.

**Software Inventory**

The Software Inventory section of client settings controls how software inventory is collected. It is enabled by default with the schedule of every seven days.

It is recommended that the schedule be changed to every one days, to ensure that software reporting is as current as possible.

Unfortunately, in SCCM 2012 the inventory file types is blank. This means that no files will be inventoried by default. In previous versions of SCCM, all EXE files were inventoried out of the box. It is recommended that organizations inventory at a minimum all EXE (*.exe), all DLL (*.dll), and all PST (*.pst) files. Figure 3.18 shows the recommended file inventory types.
FIGURE 3.18 The recommended file inventory types.

**Software Metering**

In the Software Metering section, the only settings are to enable software metering and for the deployment reevaluation schedule. This defaults to seven days and should be adjusted to every one day, if the feature is enabled.

**Software Updates**

The Software Update section of client settings controls updates behavior. It is enabled by default, but there are several schedule options within the section that should be adjusted.

The software update scan schedule defaults to every seven days, but should be adjusted to every one days. This allows much more timely information to be collected, such as what updates have been applied. This is reflected in reports, which will be current as of the previous day.

The scheduled deployment reevaluation schedule defaults to every seven days and should be left as is. The schedule determines how often the agent checks to see if it is still in compliance with previous deployments, which might result in updates being deployed.

The next setting controls what the agent does when a particular software update deployment deadline is reached, should the agent also opportunistically install any other pending software update deployments. And it allows how far in advance to look for pending software update deployments. Because update deployments frequently result in reboots, it makes sense to deploy future updates at the same time.
The setting defaults to False, so it is recommended to change that to True and the next setting to seven days. This ensures that any updates with mandatory deadlines scheduled up to a week in advance will be deployed at the same time.

**State Messaging**

The State Messaging section of client settings controls a little-known, but key aspect of the Configuration Manager agent. As the agent is executing policy, deployments, and tasks, it generates status messages and delivers them to the server to be stored in the database.

The State Messaging section controls the frequency with which those messages get uploaded. The default is every 15 minutes, but can be adjusted depending on conditions.

**User and Device Affinity**

The User and Device Affinity section of client settings controls a much requested feature that Configuration Manager 2012 delivers. Device affinity allows devices such as desktops and laptops to be associated with their users. In SCCM 2012, this can be done automatically.

In the User and Device Affinity section, administrators can specify how much time a user needs to spend with the device for it to be automatically associated with the user account.

There are two threshold settings that create the automatic association. The first is the User Device Affinity Usage Threshold (min) setting, which sets how much time a user needs to spend using the machine for it to be considered associated with that user. The second is the User Device Affinity Usage Threshold (days) setting, which sets the span of time over which usage is measured.

To enable User and Device Affinity, the Automatically Configure User Device Affinity from Usage Data setting needs to be set to True.

In addition, the Allow Users to Define Their Primary Devices setting allows users to actually specify their primary device (that is, set the affinity). It is recommended that this be set to True to give users control.

Figure 3.19 shows the recommended User and Device Affinity settings.
Configuring the Client Installation Settings

In Configuration Manager 2012, the client push installation settings are associated with each primary or secondary site in the hierarchy. The Client Installation Settings menu for each site holds the two installation options: Client Push Installation and Software Update-Based Client Installation. The Client Push Installation option is typically used to perform client deployments. The settings within the Client Push Installation configure the command-line options used when the client is pushed, the account used to access the remote computer, and if one of the Configuration Manager discovery methods triggers an installation of the client on remote systems.

A client can be pushed manually from the Configuration Manager console or executed automatically when a Discovery Method is executed. It is important to disable the Automatic Push Installation option until the client is tested and the correct options are set.

To configure the Client Installation account, complete the following steps:

1. Open the console, browse to Administration, expand Site Configuration, expand Sites, and select SFO Site.

2. Right-click on SFO Site and select Client Installation Settings, Client Push Installation.

3. Check the Enable Automatic Site Wide Client Push Installation check box.
4. Select the Accounts tab, click “**”, and then click New Account.

5. Add an account with local administrative rights to the systems.

6. Select the Installation Properties tab. The current installation property is SMSSITECODE=SFO.

7. Add FSP=CM2 to the Installation properties. This specifies the fallback status point for clients. Separate the properties with a space.

8. Apply the changes.

This account will be used to push the Configuration Manager agent to client systems. The SMSSITECODE=SFO command is configured by default to set the agent’s assigned site. If the agent is being pushed from a primary site, but will be managed by a different primary site or secondary site, this value should be changed to SMSSITECODE=AUTO, allowing the client to choose the correct site code based off of the configured boundaries.

Repeat the previous steps for each primary site and secondary site that will be pushing out agents.

### Implementing Internet-Based Client Management

Internet-based client management in Configuration Manager 2012 is really just configuring key roles to support the secure HTTPS protocol rather than the insecure HTTP protocol. That said, considerable preparation work needs to be done to implement the Public Key Infrastructure and certificates to support this change efficiently and effectively.

#### Creating a Public Key Infrastructure

A Public Key Infrastructure (PKI) is an important aspect of the Configuration Manager 2012 implementation. When a certificate is issued, its usage is governed by an Object Identifier (OID). A certificate can have more than one OID, essentially allowing the certificate to be used for more than one purpose.

A certificate with the Client Authentication OID is required on all managed clients, including mobile devices, to communicate with a Configuration Manager site via HTTPS.

A certificate with the Server Authentication OID (1.3.6.1.5.5.7.3.1) and Client Authentication OID (1.3.6.1.5.5.7.3.2) is required on all Configuration Manager 2012 Site Systems, including Site Servers, Management Points, Distribution Points, Software Update Points, and State Migration Points. The Server Authentication certificate is used on each Site Server to encrypt communication between the managed systems and the Configuration Manager component.

#### Deploying an Active Directory Enterprise Root CA

This example details the steps required to deploy an Enterprise Root CA in the Company ABC domain. When an Enterprise Root CA is configured, all clients in the domain automatically trust certificates issued from this CA.
All Configuration Manager Site Servers and managed clients must trust the Certificate Authority. Any Configuration Manager Site Servers or managed clients that don’t trust this Certificate Authority will not communicate with the infrastructure and might become orphaned. This typically happens when non-domain member servers, such as bastion hosts in the demilitarized zone (DMZ), are not part of the domain but have a Configuration Manager agent installed. To correct this problem, install the CA certificate into the local computer’s Trusted Root Certificate Authorities certificates store.

**NOTE**

Status messages will still be sent to the Fallback Status Point, even if the client system has become orphaned due to certificate configuration issues. It is important to deploy the Fallback Status Point before deploying clients.

To deploy an Enterprise Root CA, complete the following steps:

1. Open the Server Manager console on CERT, the intended CA server.
2. Select the Roles node.
3. Click the Add Roles action.
4. Click Next to skip the Roles Overview page.
5. Enable the Active Directory Certificate Services role, and then click Next.
6. Click Next to skip the AD CS overview page.
7. Enable the Certification Authority role service.
8. Enable the Certification Authority Web Enrollment role service.
9. Click Add Required Role Services when prompted, and then click Next.
10. Select Enterprise and click Next.
11. Select Root CA and click Next.
12. Select Create a New Private Key and click Next.
13. Accept the default Cryptography settings and click Next.
14. Accept the default CA Name settings and click Next.
15. Accept the default Validity Period settings and click Next.
16. Accept the default Certificate Database Location settings and click Next.
17. Click Next to skip the IIS Overview page.
18. Accept the default IIS Role Services and click Next.
19. Confirm the installation selections and click Install.
20. Wait for the installation to complete and click Close.
After implementing the CA, the CRL Distribution Point (CDP) settings need to be configured to allow HTTP access to the CRL files. For security reasons, this typically wouldn’t be done on the issuing CA; the CRL would be published on a system designated for that role. However, for demonstration purposes, the CRL will be published on the server CERT, allowing Internet-based clients to check the CRL.

To publish the CRL, complete the following steps:

1. Open the Server Manager console on CERT.
2. Expand the Roles node.
3. Expand the Active Directory Certificate Services node.
4. Right-click companyxyz-CERT-CA and click Properties.
5. Select the Extensions tab.
6. Select http://<ServerDNSName>/CertEnroll/<CaName>... from the list of CDPs.
7. Enable Include in CRLs. Clients use this to find Delta CRL locations.
8. Enable Include in the CDP Extension of Issued Certificates.
9. Apply the changes, click Yes when you are prompted to restart the Active Directory Certificate Services, and then click OK to close the window.

**Validating the Enterprise Root CA**

The newly installed Enterprise Root CA should be validated before certificates are issued to clients. To validate the CA, check the local application event log on the server CERT. This can be accessed through the Diagnostics node of Server Manager.

If the application event log is clean and doesn’t contain any error or warning messages about Certificate Services or related components, the server should be ready to issue certificates to clients. It is always a good practice to restart the certificate server to ensure the Certificate Services can start and stop without logging any issues. It is also important to resolve all problems before moving to the next section and deploying certificates to managed clients and Site Servers.

**Deploying Certificates**

An enterprise Certificate Authority simplifies management of certificates by providing a secure, scalable certificate provisioning process through Active Directory. This task assumes all of the Configuration Manager servers and the Enterprise Root CA server have been moved to an organizational unit (OU) called Servers, and all of the workstations have been moved to an OU called Workstations.

The Servers and Workstations OUs are child objects of an OU called Managed. The Managed OU is located in the root of the domain.
CAUTION

Do not move domain controllers from the default OU. Moving domain controllers out of the default Domain Controllers OU is not supported.

When an Enterprise Root CA is deployed, all domain controllers automatically receive a “Domain Controller” certificate. This certificate can be used for both client and server authentication.

Configuring the Auto-Enrollment Group Policy Object

A Group Policy Object (GPO) called Certificate Auto-Enrollment will be created and linked to the Servers OU and the Workstations OU. This group policy will be used to enable the certificate auto-enrollment function for all managed systems.

To create the Certificate Auto-Enrollment GPO, complete the following steps:

1. Open the Group Policy Management Console on DC1.
3. Expand Domains.
5. Select the Group Policy Objects container.
6. Right-click the Group Policy Objects container and select New.
7. Enter Certificate Auto-Enrollment in the Name field and click OK.

Once the GPO has been created, the setting that allows Certificate Auto-Enrollment can be enabled.

To enable the Certificate Auto-Enrollment setting in the GPO, complete the following steps:

1. Right-click the Certificate Auto-Enrollment GPO and select Edit.
2. The Group Policy Management Editor opens.
5. Expand Windows Settings.
7. Select the Public Key Policies container.

   The Certificate Services Client - Auto-Enrollment location is shown in Figure 3.20.
9. Select Enabled as the Configuration Model.

10. Enable the option to Renew Expired Certificates.

11. Enable the option to Update Certificates That Use Certificate Templates.

12. **Click OK** to save changes and close the Group Policy Management Editor.

Once the Auto-Enrollment setting within the GPO has been configured to allow automatic certificate enrollment, the GPO can be linked to the correct OUs.

To link the Certificate Auto-Enrollment GPO to the correct OUs, complete the following steps:

1. **Open the Group Policy Management Console.**

2. **Expand the Managed OU and select the Servers OU.**

3. **Right-click the Servers OU and select Link an Existing GPO.**

4. **Select Certificate Auto-Enrollment from the list of GPOs and click OK.**

5. **Right-click the Workstations OU and select Link an Existing GPO.**

6. **Select Certificate Auto-Enrollment from the list of GPOs and click OK.**
When this is complete, any domain member server or workstation placed in the corresponding OUs will be configured for automatic certificate enrollment. To complete the process, a certificate template with the correct settings and permissions needs to be created and then published.

**Configuring Certificate Templates**

The next step is to create certificate templates with the appropriate settings and permissions. The permissions on the certificate template govern the clients’ ability to request the certificate. This is important because only the required certificates should be deployed to the system.

**CAUTION**

Provisioning certificates with unnecessary OIDs is not recommended. Only provision the minimum requirements needed by the client to communicate with Configuration Manager.

**Creating the Client Authentication Certificate Template**

Security permissions on the certificate template for Client Authentication will be configured to allow the domain computers security group to automatically request and receive this certificate through Active Directory. All systems in the Workstations and Servers OUs will receive this certificate.

To create Client Authentication templates for auto-enrollment, complete the following steps:

1. Open the Server Manager console on CERT.
2. Expand the Roles node.
3. Expand the Active Directory Certificate Services node.
4. Select the Certificate Templates container.

   The Certificate Templates container is shown in Figure 3.21.
5. Right-click the Workstation Authentication template.
6. Select Duplicate Template.
7. Choose Windows Server 2003 Enterprise and click OK.

**CAUTION**

8. Type **Client Certificate Auto-Enrollment** in the Template Display Name field.
10. Enable the Autoenroll permission for domain computers.
11. Select the Extensions tab.
12. Select the Application Policies item.
13. Verify the description states Client Authentication.
14. Click Apply and then click OK to close the window.
Creating the OS Deployment Template

Security permissions on the certificate template for OS Deployment will be configured to only allow manual certificate requests. Before PXE Service Points are implemented, the Client Authentication OS Deployment certificate will be requested through the web enrollment page.

To create the OS Deployment template, complete the following steps:

1. Open the Server Manager console on CERT.
2. Expand the Roles node.
3. Expand the Active Directory Certificate Services node.
4. Select the Certificate Templates container.
5. Right-click the Workstation Authentication template.
6. Select Duplicate Template.
7. Choose Windows Server 2003 Enterprise and click OK.
8. Type Configuration Manager OS Deployment in the Display Name field.
9. Select the Issuance Requirements tab.
10. Enable CA Certificate Manager Approval.
11. Select the Request Handling tab.
12. Enable the Allow Private Key to Be Exported option.
13. Select the Subject Name tab.
14. Enable the Supply in the Request option.
15. Select the Security tab and remove Domain Computers from the list.
16. Click Apply and then click OK to close the window.

Creating the Server Authentication Certificate Template

Security permissions on the certificate template for Server Authentication will be configured to only allow a custom security group to automatically request this certificate through Active Directory. Ultimately, all systems that will host web services will receive this certificate.
Before executing the next task, create a universal security group called SCCM Site Servers in the domain. Add the Configuration Manager servers and the Certificate Authority server to this group.

**CAUTION**

When a computer object is added to a group, it can take a long time for the setting to take effect. This is because the Kerberos ticket takes seven days to renew. The renewal time is governed by the *Maximum Lifetime for User Ticket Renewal* setting located in the Default Domain Policy GPO. It is not recommended to change this setting. Instead, restart the computer to refresh the Kerberos ticket.

To create Server Authentication template for auto-enrollment of the SCCM Site Servers, complete the following steps:

1. Open Server Manager and expand Roles, expand Active Directory Certificate Services, and select the Certificate Templates container.

2. Right-click the Workstation Authentication template.

3. Select Duplicate Template.

4. Choose Windows Server 2003 Enterprise and click OK.

5. Type **Server Certificate Auto-Enrollment** in the Display Name field.


7. Remove the Domain Computers security group.

8. Click Add, type the group **SCCM Site Servers**, and then click OK.

9. Highlight SCCM Site Server.

10. Uncheck the Read permission.

11. Check the Enroll and Autoenroll permissions.

The permission for this certificate is shown in Figure 3.22.
12. Select the Extensions tab.

13. Select the Application Policies extension item and click Edit.

14. Highlight the Client Authentication Policy and click Remove.

15. Click Add, choose Server Authentication from the list, and then click OK.

16. Click OK, click Apply to apply the settings, and close the window.

All servers that are added to the Servers OU and are members of the SCCM Site Servers security group will receive a certificate that can be used for server authentication.

**Publishing the Certificate Templates**

Now that the Client and Server Authentication certificates have been created, they can be published. This tells the Certificate Authority the template is available for client consumption.

To publish the authentication templates for auto-enrollment, complete the following steps:

1. Open Server Manager on CERT.

2. Expand Roles.
4. Expand companyxyz-CERT-CA.
5. Select the Certificate Templates container.

The CA Certificate Templates container is shown in Figure 3.23.

![Certificate Templates container](image)

**FIGURE 3.23** The CA Certificate Templates container.

7. Click New and then click Certificate Template to Issue.
8. Select the Client Certificate Auto-Enrollment template from the list.
9. Hold down the Ctrl key.
10. Select the Server Certificate Auto-Enrollment template from the list.
11. Select the Configuration Manager OS Deployment template from the list.
12. Click OK to complete the process.

The three certificates should be listed in the Certificates Template container for the CA. These certificates are ready for consumption by Configuration Manager Site Servers and managed clients.
Configuring the Certificate Services Website for SSL

Certificates cannot be issued with the Certificate Services Enrollment web server unless it is configured to use SSL. This section describes the steps needed to secure the website with a server certificate. This also validates the ability for the certificate server to issue certificates.

To configure the Certificate Services website for SSL, complete the following tasks:

1. Open the command prompt on CERT.
2. Type `gpupdate /force` to refresh the group policies.
3. After the group policy is refreshed, open Server Manager.
4. Expand Roles.
6. Expand companyxyz-CERT-CA.
7. Select the Issued Certificates container.

The two new certificates should be listed in the container.

The CA Issued Certificates container is shown in Figure 3.24.

![Figure 3.24 The CA Issued Certificates container.](image)

The server CERT has received both the client and server signing certificate. The server signing certificate can be used to secure the Certificate Services website.
To secure the Certificate Services website, complete the following steps:

1. Open the Server Manager on CERT.
2. Expand Roles.
3. Expand Web Server (IIS).
4. Select Internet Information Services.
5. Expand the CERT web server.
7. Select Default Web Site.
8. Select Bindings from the Actions pane.
9. Click Add.
10. Select HTTPS for the binding type.
11. Select the correct certificate from the SSL certificate menu.
12. Click View to verify the correct certificate has been selected and then click OK.
13. Click OK and then click Close.

To test the newly installed certificate, open Internet Explorer and browse to the URL https://cert.companyxyz.com/certsrv. The Certificate Enrollment web page should open. Click the small lock icon beside the address bar, which shows the status of the certificate and that the Certificate Authority companyxyz-CERT-CA has identified this computer as cert.companyabc.com.

**Configuring the WSUS Website for SSL**

Because the WSUS component was installed on the CM1 server, the same certificate that was used to secure the Default Site can be used to secure the WSUS Administration site from within IIS.

**CAUTION**

Do not enable all virtual directories within the WSUS Administration site to use SSL. Only the APIRemoting30, ClientWebService, DSSAuthWebService, ServerSyncWebService, and SimpleAuthWebService should require SSL.

To configure WSUS for SSL communication, complete the following steps:

1. Open Internet Information Services Manager.
2. Expand Sites, and select the WSUS administration site, which is often the Default Web Site.
3. Click the Bindings action.
4. Click Add, select HTTPS, and click Edit.

5. Choose the certificate from the list.

6. Click View to verify the correct certificate was selected, click OK, and then click Close.

7. Select the APIRemoting30 virtual directory.

8. Double-click the SSL Settings option.

9. Enable the Require SSL option and click Apply.


When the WSUS virtual directories are correctly configured, run the following command on the WSUS server to finalize the configuration needed to support SSL:

```
WSUSUtil.exe configuressl cm1.companyxyz.com
```

This utility is located in the Tools folder located within the WSUS installation folder. By default, this is folder is `c:\Program Files\Update Services\Tools`.

**Requesting the OS Deployment Certificate**

The OS Deployment client certificate is used by all systems during the OS deployment. This is essentially a shared certificate that is imported when the PXE Service Point is established.

The same procedure used to request the Document Signing certificate can be used to request the OS Deployment certificate. The main differences are instead of selecting the Configuration Manager Document Signing template from the template list, the Configuration Manager OS Deployment template must be selected. In the Name field, enter `osd01.companyxyz.com`.

**NOTE**

This certificate does not need to be added to the Local Computer certificate store. The Personal Information Exchange (PFX) file created will be imported during the deployment of the PXE Service Point detailed later.

Remember to approve the certificate `osd1.companyxyz.com` from within the Pending Requests container. When exporting the certificate, enter `c:\Temp\OSD01.pfx` as the file.

**Enabling Internet-Based Client Management**

In Configuration Manager 2012, the Site Servers roles have to be explicitly configured to enable Internet-based client management (IBCM). Each Management Point and Distribution Point that are to be enabled for IBCM will need to be configured to communicate over
HTTPS rather than HTTP. This is typically done on one or more systems dedicated to handling Internet traffic, but the actual configuration can depend on specific business and security requirements.

When a client communicates over the Internet, it needs to communicate with the following:

- Management Point
- Distribution Point
- Software Update Point
- Fallback Status Point
- Enrollment Proxy Point
- Application Catalog Website Point

All communication is done over HTTPS, with the exception of the Fallback Status Point, which communicates over HTTP. The first step in the process is to enable IBCM on the Site Server.

The FSP and SUP do not require additional configuration and are automatically enabled with the Site Server. Finally, to support IBCM, the following ports need to be open from the Internet:

- CRL Web Site: TCP 80
- Fallback Status Point: TCP 80
- Management Point: TCP 443
- Distribution Point: TCP 443
- Software Update Point: TCP 443

It is not recommended to connect any internal system directly to the Internet; for production deployments, consider using a reverse proxy, such as the Microsoft Threat Management Gateway (TMG).

Summary

System Center Configuration Manager 2012 provides a scalable, secure, end-to-end administration and reporting functionality. The deployment can be scaled out over many servers to support hundreds of thousands of managed clients, or installed on a single server for small enterprise deployments. In both cases, it is important to understand how each of the Configuration Manager roles work and the required dependencies for each role so the implementation is successful.
Best Practices

The following are best practices from this chapter:

- It is important to fully understand the architectural design before Configuration Manager 2012 server infrastructure servers and roles are deployed.

- If communication issues are a problem, make sure the settings on the local firewall have been configured correctly. For troubleshooting purposes, disable the local firewall temporarily.

- Status messages will still be sent to the Fallback Status Point, even if the client system has become orphaned due to certificate configuration issues. It is important to deploy the Fallback Status Point before deploying clients.

- Do not move domain controllers from the default OU. Moving domain controllers out of the default Domain Controllers OU is not supported. When an Enterprise Root CA is deployed, all domain controllers automatically receive a Domain Controller certificate. This certificate can be used for both client and server authentication.

- Provisioning certificates with unnecessary OIDs is not recommended. Only provision the minimum requirements needed by the client to communicate with Configuration Manager.


- When a computer object is added to a group, it can take a long time for the setting to take effect. This is because the Kerberos ticket takes seven days to renew. The renewal time is governed by the Maximum Lifetime for User Ticket Renewal setting located in the Default Domain Policy GPO. It is not recommended to change this setting. Instead, restart the computer to refresh the Kerberos ticket.

- Make sure the subject name of the Site Servers’ Document Signing certificate is set to: The site code of this Site Server is <SITE CODE>. The <SITE CODE> represents the site code that will be entered during the Configuration Manager implementation.

- Review the ExtADsch.log file for any errors after the AD schema has been extended. This log file is located in the root of drive C on the server used to execute the schema extensions. The log file should show 14 attributes and four classes have been defined.

- Do not bother with the WSUS Configuration Wizard. When the wizard opens after WSUS is successfully installed, click the Cancel button. The Configuration Manager console provides the interface to configure synchronization with Microsoft.
Make sure the Configuration Manager Site Server Computer Account is in the local administrators group on all component servers and other Site Servers; this includes the Site Database server. The computer account of the Site Server is used to access and manage the remote server by default.

The status summarizer for the different components is not automatically changed from red or yellow to green if the component that experienced the problem is fixed. The component summarizer simply counts the number of warning and error status messages that have been received. Manually reset the counts of status messages to clear the error or warning status.

The cmtrace.exe log viewer provides a real-time view of the Configuration Manager status logs. This tool is invaluable when troubleshooting problems and understanding the environment.

When deploying Site System roles to either the Site Server or a remote server, it is important to note the component installation wizard doesn’t actually do the installation. Check the Site Status container from within the console along with the local installation logs for details on role installation.

Increase the number of messages allowed per hour by the FSP to support large client deployments. This prevents a backlog of status messages from occurring.

Never configure overlapping boundaries. This can cause managed systems to use the wrong Site Server or Distribution Point. This often happens when using a combination of IP and Active Directory boundaries.

Define the Network Access Account on the Computer Client Agent when managing non–domain members. This account is provided as a way for non–domain members to authenticate to Configuration Manager. This account should be a Domain User without additional permissions.

The default list of “Products” supported by the Software Update Point is refreshed and updated during the synchronization process. This adds things like Windows 7 and Windows Server 2008 R2 to the Windows section. Because the entire Windows product was selected, new operating systems will automatically be enabled as they are made available on the Windows Update site and through WSUS.

Configuring Client Agents with a “simple” schedule allows the distribution of load placed on the system. Unless the server and environment have been sized to receive and process data from all clients simultaneously, care should be taken to distribute the load over a longer period.
This page intentionally left blank
Index

Numbers
64-bit agents, 59

A
Access Violation reports (ACS), 542
accessing Client Agents node, 248
Account Management reports (ACS), 542-543
accounts. See names of specific accounts
ACS (Audit Collection Services)
  hardware/software requirements, 311
  installing, 368-373
  overview, 310-311
  reports
    Access Violation reports, 542
    Account Management reports, 542-543
    custom reports, 545-548
    explained, 541-542
    Forensic reports, 543
    generating, 544-545
    Planning reports, 543
    Policy reports, 543
    System Integrity reports, 543
    Usage reports, 544
Action accounts, 315-316
Active Alerts, 436
Active Directory
  connectors, deploying, 805-806
  Runbook Designer, connecting to, 952
  schema, extending, 64-66, 118-119
  site detection, 60
Active Directory Client Monitoring, 453-454
Active Directory Domain Controller Performance Collection, 458-460
Active Directory forest discovery, 139
Active Directory Group Discovery, 95, 144
Active Directory Management Pack, 451
configuring, 451-460
reports, 465-466
tasks, 464
views, 460-463
Active Directory Management Pack Helper
Object installation files, 452
Active Directory Replication Monitoring, 454-458
Active Directory Server Client object
discovery, 453
Active Directory System Discovery, 143-144
Active Directory User Discovery, 144
activities
dependent activities, 886
manual activities, 886, 898
adding to change requests, 897
completing and failing, 905-907
parallel activities, 886
review activities, 886
runbook activities, 952-953
runbook automation activities, 886
Service Manager 2012, 886
Activities pane (Runbook Designer), 945
Activity Distribution report, 917
activity management reports, 917-918
activity prefixes, 888-889
Add Configuration dialog box, 952
Add Disks to Storage Pool dialog box, 592
Add Properties page (Convert Physical Server
Wizard), 723
Add Resource Wizard, VMM Agent installation,
695-697
Additional Properties page (Convert Virtual
Machine Wizard), 728
administration
DPM (Data Protection Manager)
custom volumes, 613-614
data recovery, 614-616
DPM Administrator Console, 607-608
DPM Central Console, 610-613
DPM Management Shell, 608-610
guest sessions, delegating, 37
Operations Manager
dip stick health checks, 403-404
file exclusions for antivirus and defragmentation applications, 409-410
management pack updates, 404-405
notifications and alert tuning, 405-409
Web console Performance view time frame, 410-411
VMM (Virtual Machine Manager), 707-708
VMM Administrator Console, 707-715
VMM command shell, 715-716
Administration Console (DPM)
overview, 607-608
protection agent deployment, 594-596
Administrator Console (VMM), 679-680, 707-709
configuring VMM library, 710-711
creating host groups, 708-709
creating private clouds, 711-714
deploying VMs with, 742-744
explained, 668
General settings, 715
hardware requirements, 679
installing, 692-693
managing host clusters, 710
managing hosts, 709
managing VMs, 714
monitoring and reporting, 714
Security settings, 715
software requirements, 680
supported operating systems, 680
System Center settings, 715
Administrator Properties dialog box, 731
Administrator role (Operations Manager), 312
Administrator role (VMM), 672, 729-731
Advanced Operator role (Operations
Manager), 312
advantages of Microsoft System Center, 6-7
Agent (VMM), installing, 695-700
Agent Action accounts, 316
Agent Compliance report, 284
Agent Health State, 437
Agent Performance dashboard, 435-436
Agent Proxy configuration, 396-398
Agent State Dashboard view, 437
agents, 99
64-bit agents, 59
automatic upgrades, 59
Operations Manager agents, 373
audit forwarders, configuring, 376-379
configuring to use certificates, 392
installing on DMZ servers, 391-392
security, 313
UNIX/Linux agents, installing, 379-385
Windows agents, installing, 373-376
overview, 298-299
protection agents, deploying
  with certificates, 599-601
  with DPM Administration Console, 594-596
  manual installation process, 596-599
  with PowerShell, 601
proxy agents, configuring, 396-398
pushing, 59
Restart Health Service Recovery, enabling, 398-399
Server App-V Agent
  definition of, 753
  installing, 754-755
  supported operating systems, 298
VMM Agent
  explained, 668
  installing, 695-700
AI (Asset Intelligence), 72-73, 269
  importing software license data, 275-277
  reporting, 277
  reporting classes, 270-274
  synchronizing, 269-270
Alert Logging Latency report, 534-536
alert widgets
  adding to dashboards, 558
  explained, 556
alerts
  generating, 294
  overview, 292
  state-based alerting, 59
  tuning, 405-409
Alerts reports (Operations Manager), 525-527
All Application Deployments (Basic) report, 253
All Audit Messages for a Specific User report, 254
All Management Servers Resource Pool, 318
All Software Updates container, 68
All Task Sequence Deployments report, 254
analyzing
  incidents, 847-849
  problems, 860-861
announcements, publishing, 850
antivirus applications, file exclusions for, 409-410
Application Catalog Web Services Points, 58
Application Catalog Website Points, 58
Application Compliance report, 253
application deployment, reports, 253
application management (Configuration Manager), 59, 66-68, 189. See also deployment management
  application model, 67-68, 189-190
  complex application configuration, 196
  complex application creation, 198-202
  complex application installation automation, 197-198
  distributing content to Distribution Points, 202-203
  EXE application configuration, 192-196
  MSI application configuration, 191-192
  package model, 67, 190-191
  targeting deployments to primary systems, 200-202
application model (application management), 67-68, 189-190
applications, 67-68
  monitoring, 21, 290
  preparing for OS deployment, 227
  virtual application packages
    creating, 755-758
    definition of, 753
    importing into VMM, 758
approving RAs (review activities), 903-905
architecture
  Configuration Manager, 75-76
  multisite Configuration Manager hierarchy, 95-96
  Operations Manager, 296-298, 317
  Service Manager, 766-767, 830-832
asset data, 246
  IDMIF files, 247
  inventory collection, 246-247
  NOIDMIF files, 247
Asset Intelligence. See AI (Asset Intelligence)
Asset Intelligence Synchronization Point role, 269-270
  installing, 153-154
  overview, 81-82
asset management (Configuration Manager), 70
  Asset Intelligence. See AI (Asset Intelligence)
  Compliance Management, 73-74
  hardware and software inventory, 71
  software metering, 73
asset tracking, 12
assigning incidents, 846-847
audit collection database, 309-310
Audit Collection Services. See ACS
audit collectors, 309
audit forwarders, 308, 376-379
auditing reports (Configuration Manager), 254
auditing review, 48
Author role (Operations Manager), 312
Authoring Console, 503
automatic agent upgrades, 59
automatic deployment rules, 69, 222-224
automatic deployments, 211-213
automatic load balancing, 58
Automatic Placement (VMM), 741
automatic user notification, change requests, 908-910
automating complex application installation, 197-198
Availability reports (Operations Manager), 527-531
Availability Tracker report, 528

B
Back Up Database dialog box, 412-416, 815
Background Intelligent Transfer Service. See BITS
Backup Destination dialog box, 414
backups
cloud backups, 31
database backups, 30
Hyper-V server backups, 31
Microsoft server backups, 28
Operations Manager backups, 321-322
component backup schedules, 411-412
IIS 7.x configuration backup, 417-418
OperationsManager database, 412-414
OperationsManagerAC database, 416-417
OperationsManagerDW database, 414-415
server backups, 29
Service Manager backups, 814
backup schedules, 814
database backups, 814-816
encryption key, 816-817
SharePoint data backups, 30
Site Server database backups, 81
SQL backups, 30
tape backups, 31
limitations of, 569-570
bandwidth
Operations Manager requirements, 325-326
site deployment and, 96
baselines, 283
benefits of Microsoft System Center, 6-7
best practices
Configuration Manager, 112-114, 178-179
deployment management, 243-244
DPM (Data Protection Manager), 617-618, 661-662
Operations Manager, 354, 418-419, 566
Service Manager, 817-818, 870
System Center Orchestrator, 968
VMM (Virtual Machine Manager), 701-702, 759-760
BITS (Background Intelligent Transfer Service)
client settings, 100, 156
troubleshooting, 138
BITS-enabled Distribution Points, 83-84
boot images
managing, 231
MDT boot images, creating, 240
boundaries
configuring, 139-143
establishing, 97-99
explained, 61
boundary groups, configuring, 139-143
Branch Distribution points, 59
BranchCache, 84
building runbooks
Copy File and Log Event runbook, 953-959
Move Disabled Users runbook, 962-965
business solutions, addressing
Configuration Manager, 10
DPM (Data Protection Manager), 28
Operations Manager, 19-20
Orchestrator, 46-47, 922
Service Manager, 41
VMM (Virtual Machine Manager), 35-36, 664-665
C

calculating storage requirements for DPM (Data Protection Manager) deployment, 585

cancelling change requests, 900-901, 903

Capacity Planner, 9

captured data, storing, 329

capturing existing user state, 231

CDP (continuous data protection), 571-572

CEC (Common Engineering Criteria), 421

Central Administration Site, 15, 57, 124
database, 246
installing, 124-126
validating installation, 127-129

Central Administration Site Servers, 77-78

Central Console (DPM), 610-613

Certificate Auto-Enrollment GPO, configuring, 166-168

certificate requirements (IBCM), 108-109

Certificate Services website, configuring for SSL, 174-175

certificates
deploying, 165
Enterprise Root CA, 163-165
monitoring DMZ servers with, 385-386
agent configuration, 392
agent installation, 391-392
certificate templates, creating, 386-387
root CA server certificates, requesting, 387-390

OS Deployment certificate requests, 176

protection agents, deploying with, 599-601
root CA server certificates, requesting, 387-390

security DMZ servers with, 316
templates, 109-110
creating, 168-172, 386-387
publishing, 172-173

CFS (Clustered File System), 676

deleting, 913-914
restoring, 914
searching, 911-912

Citrix XenServer, VMM support for, 670

client agents
Configuration Management client agents, 278
configuring software metering, 278

Client Agents node, accessing, 248

How can we make this index more useful? Email us at indexes@samspublishing.com
Client Authentication certificate template, creating, 168-169
client certificates, 109
client configuration settings, 156
  Background Intelligent Transfer settings, 100, 156
  client installation settings, 162-163
  client policy settings, 156
  Compliance settings, 100, 156
  Computer Agent settings, 100, 157
  Computer Restart settings, 100, 157
  Endpoint Protection settings, 100, 157-158
  Hardware Inventory settings, 100, 158
  Remote Tools settings, 100, 158-159
  Software Deployment settings, 101, 159
  Software Inventory settings, 101, 159-160
  Software Metering settings, 101, 160
  Software Update settings, 160-161
  State Messaging settings, 161
  User and Device Affinity settings, 161-162
client installation settings, 162-163
Client Performance report, 477
Client Policy section (client settings), 100
client policy settings, 156
Client Push Installation account, 91
Client Push Installation Status Details report, 254
Client Push Installation Status Summary report, 254
client roaming, 65-66, 182-183
client schedules, 105-106
client settings (Configuration Manager)
  adding hardware class, 266
  configuring for inventory collection, 248-249
  planning, 99-101
Client Status History report, 254
Client Status Summary report, 254
client-side monitoring scripts, 452
clients (Configuration Manager)
  configuring. See client configuration settings
discovering and deploying, 94-95
  explained, 62
HTTP and HTTPS client connections, 12
IBCM (Internet-based client management), 106-107, 163
  Certificate Auto-Enrollment GPO configuration, 166-168
certificate deployment, 165
  Certificate Services website, configuring for SSL, 174-175
certificate requirements, 108-109
certificate templates, 109-110, 168-173
client site assignment, 108
content distribution, 184
enabling, 176-177
Enterprise Root CA, 163-165
limitations of, 107
OS Deployment certificate requests, 176
PKI creation, 163
planning PKI, 109
planning site system placement, 107-108
WSUS website, configuring for SSL, 175-176
monitoring, 20-21
overview, 76-77
Registry keys, creating, 261-262
Clients That Have Not Reported Recently (in a Specified Number of Days) report, 254
closing change requests, 907-908
cloud computing
  backing up to cloud, 31
  VMM private clouds
    creating, 711-714
    explained, 704
    fabric resources, 704
    networks, 706
    servers, 705
    storage, 706-707
Clustered File System (CFS), 676
clusters
  database, 319-320
  file server clusters, protecting data on, 622
  host clusters, managing, 710
  VMM (Virtual Machine Manager) support for, 671
CMDB (configuration management database), 765, 911
cmdlets, 716
cmtrace.exe log viewing utility, 128, 133
collections, 89
  creating, 204
  defining, 185-188
designing, 94
  maintenance windows, 187
  update schedules, 187
command line, sealing management packs, 507
command shell, 422
  Operations Manager, 306-307
  VMM, 715-716
Common Engineering Criteria (CEC), 421
compiling configuration.mof files on test clients, 265
completing manual activities, 905-907
complex applications
  automating installation, 197-198
  configuring, 196
  creating, 198-202
compliance
  monitoring, 283
  service offerings, 874
Compliance 1 - Overall Compliance report, 253
Compliance 2 - Update Group report, 253
compliance management, 12, 73-74
Compliance Settings (Configuration Manager clients), 60, 100, 156, 278
  applying baselines to collections, 283
  client agents, 278
  configuration baselines, defining, 282-283
  configuration items to monitor, defining, 278-282
Computer Agent section (client settings), 100, 157
Computer Details report, 918
Computer Inventory report, 918-919
Computer Management, 438
Computer Restart section (client settings), 100, 157
computer$ account, 95
Computers That Have a Metered Program Installed but Have Not Run the Program Since a Specified Date report, 278
Computers with a Specific File report, 253
Concurrent Usage for All Metered Software Programs report, 254
ConfigMgr. See Configuration Manager
configuration baselines, defining, 282-283
Configuration Changes report, 528
configuration items. See CI (configuration items)
configuration management database (CMDB), 765, 911
configuration management reports, 918-919
Configuration Manager, 8, 14, 245
  Active Directory schema extensions, 64-66
  administration best practices, 178-179
application management, 189
  application model, 189-190
  complex application configuration, 196
  complex application creation, 198-202
  complex application installation
    automation, 197-198
    distributing content to Distribution Points, 202-203
  EXE application configuration, 192-196
  MSI application configuration, 191-192
  package model, 190-191
architecture, 75-76
AI (Asset Intelligence), 72-73, 269
  importing software license data, 275-277
  reporting, 277
  reporting classes, 270-274
  synchronizing, 269-270
Asset Intelligence Synchronization Points, 81-82
asset data, 246-247
asset management, 70. See also AI (Asset Intelligence)
  Compliance Management, 73-74
  hardware and software inventory, 71
  software metering, 73
  best practices, 112-114
  boundaries, establishing, 97-99
  business solutions addressed by, 10
Central Administration Site, 124
  installing, 124-126
  validating installation, 127-129
Central Administration Site Servers, 77-78
client configuration, 156
  Background Intelligent Transfer settings, 100, 156
  client installation settings, 162-163
  client policy settings, 156
  Compliance settings, 100, 156
  Computer Agent settings, 100, 157
  Computer Restart settings, 100, 157
  Endpoint Protection settings, 100, 157
  Software Deployment settings, 101, 159
  Software Inventory settings, 101, 159

How can we make this index more useful? Email us at indexes@samspublishing.com
Software Metering settings, 101, 160
Software Update settings, 160-161
State Messaging settings, 161
User and Device Affinity settings, 161-162
client schedules, 105-106
client settings
configuring for inventory collection, 248-249
planning, 99-101
clients
discovering and deploying, 94-95
overview, 76-77
collections
defining, 185-188
designing, 94
Compliance Settings, 278
applying baselines to collections, 283
client agents, 278
defining configuration baselines, 282-283
defining configuration items to monitor, 278-282
connectors, deploying, 811-812
content distribution, 181
application management, 66-68
client roaming, 182-183
Distribution Point selection, 184-185
for Internet-based clients, 184
operating system deployment, 69-70
software update distribution, 68-69
customizing hardware Inventory, 261
adding hardware class in client settings, 266
creating Registry keys on the client, 261-262
editing configuration.mof files, 263-265
manually compiling configuration.mof on test clients, 265
validating custom inventory data, 267-268
viewing custom inventory data, 268
data flow, 101-102
database sizing, 93
deployment management
automatic deployments, 211-213
best practices, 243-244
monitoring deployments, 213-215
self-service deployments, 207-211
targeting users, 203-207
design scenarios
large enterprises, 111-112
small and medium enterprises, 110-111
disk subsystem performance, 102
SAN versus DAS, 102-104
SQL versions, 104-105
Distribution Points
BITS-enabled Distribution Points, 83-84
BranchCache features, 84
overview, 82-83
protected Distribution Points, 84
SMB-based Distribution Points, 83
Fallback Status Point (FSP), 84
hardware requirements, 92-93
health reports, 254
Health Validator Point, 85
hierarchy configuration, 62-63, 138
boundaries and boundary groups, 139-143
discovery methods, 143-144
Exchange connectors, 147-148
hierarchy and geographic views, 145-147
how it works, 60-62
IBCM (Internet-based client management), 106-107, 163
Certificate Auto-Enrollment GPO configuration, 166-168
certificate deployment, 165
certificate requirements, 108-109
Certificate Services website, configuring for SSL, 174-175
certificate template creation, 168-172
certificate template publication, 172-173
certificate templates, 109-110
client site assignment, 108
enabling, 176-177
Enterprise Root CA, 163-165
limitations of, 107
OS Deployment certificate requests, 176
PKI creation, 163
planning PKI, 109
planning site system placement, 107-108
WSUS website, configuring for SSL, 175-176
installation prerequisites, 118
  adding Windows roles on Site Servers, 121-124
  configuring System Management container, 120-121
  extending Active Directory schema, 118-119
major features of, 11:12
Management Points, 85-86
MDT (Microsoft Deployment Toolkit), 238
  creating task sequences, 240-242
  installing, 238
  integrating together, 239-240
Mobile Device Management, 87-88
MOF files, editing, 261
monitoring baselines and compliance, 283
multisite hierarchy, 95-96
new features, 15-17, 56
  administration changes, 60
  console redesign, 56
  hierarchy changes, 56-57
  operations changes, 59-60
  Site System role changes, 58-59
OS deployment, 225-227
  application and deployment type preparation, 227
  boot image management, 231
  creating operating system install task sequences, 231-234
  creating task sequence deployment, 235-236
  creating User State Migration package, 227-228
  driver management, 230-231
  importing unknown computers, 234-235
  monitoring, 236-238
  operating system image management, 229-230
  operating system installer management, 228-229
  scenarios for, 226-227
  technologies for, 225-226
Out-of-Band Service Points, 86
Primary Site Servers
  installing, 129-131
  overview, 78
  validating installation, 131-133
PXE-enabled Distribution Points, placement of, 97
reporting, 249
Reporting Service Point (RSP), 87
  reports, 74-75
  editing, 256-261
  generating, 250-252
  lists of, 252-255
  scheduling, 255-256
revisions and product history, 13-15
sample organization in illustrations, 115-117
secondary sites, 64
  installing, 134-136
  validating installation, 136-138
security, 88
  port requirements, 89-90
  role-based administration, 89
  for server communication, 88-89
  service accounts, 91
site configuration, 148
  Asset Intelligence Synchronization Point role installation, 153-154
  Endpoint Protection Point role installation, 152-153
  FSP (Fallback Status Point) installation, 149
  OS deployment preparation, 154-155
  RSP (Reporting Service Point) installation, 149-150
  Software Update Point role installation, 150-152
Site Server database, 79-81
SMS Providers, 78-79
software metering, 277-278
software requirements, 93
Software Update Point (SUP), 87
State Migration Point (SMP)
  overview, 86-87
  placement of, 97
  update deployment, 219
  automatic deployment rules, creating, 222-224
  deployment packages, creating, 219-220
  monitoring, 224-225
  Software Update deployments, creating, 220-222

How can we make this index more useful? Email us at indexes@samspublishing.com
update management, 215
   creating software update groups, 216-219
   viewing Update Repository, 215-216
   Wake On LAN functionality, 81
configuration.mof file, 263-265
Configure Orchestrator Users Group screen
   (Orchestrator Setup Wizard), 931
Configure the Database screen (Orchestrator
   Setup Wizard), 931
Configure the Ports for the Web Services screen
   (Orchestrator Setup Wizard), 932
Configure the Service Account screen
   (Orchestrator Setup Wizard), 931
ConfigureSharePoint.exe utility, 645
configuring. See also deploying
   Active Directory Client Monitoring, 453-454
   Active Directory Domain Controller
      Performance Collection, 458-460
   Active Directory Forest Discovery, 139
   Active Directory Management Pack, 451-460
   Active Directory Replication Monitoring,
      454-458
   agents for certificates, 392
   audit forwarders, 376-379
   Certificate Auto-Enrollment GPO, 166-168
   Certificate Services website for SSL,
      174-175
change settings, 887
   activity prefixes, 888-889
   Change Request Prefix, 887
   file attachment limits, 887-888
client settings for inventory collection,
   248-249
clients (Configuration Manager), 156
   Background Intelligent Transfer settings,
      100, 156
   client installation settings, 162-163
   client policy settings, 156
   Compliance settings, 100, 156
   Computer Agent settings, 100, 157
   Computer Restart settings, 100, 157
   Endpoint Protection settings, 100,
      157-158
   Hardware Inventory settings, 100, 158
   Remote Tools settings, 100, 158-159
   Software Deployment settings, 101, 159
Software Inventory settings, 101,
   159-160
Software Metering settings, 101, 160
Software Update settings, 160-161
   State Messaging settings, 161
   User and Device Affinity settings,
      161-162
complex applications, 196
Configuration Manager hierarchy, 138
   boundaries and boundary groups,
      139-143
   discovery methods, 143-144
   Exchange connectors, 147-148
   hierarchy and geographic views, 145-147
Cross Platform Management Packs, 487-488
DPM (Data Protection Manager)
   protection agents. See protection agents
   storage pool, 591-593
   tape libraries, 593
e-mail subscriptions for reports, 255
EXE applications, 192-196
incident settings
   file attachment limits, 822
   inbound email settings, 826-830
   incident prefix, 821
   Operations Manager Web console
      settings, 826
   priority calculation, 822-824
   resolution times, 824-825
MSI applications, 191-192
Network Access Account, 227
notifications and subscriptions, 399-402
   notification subscriptions, 834-835
   notification templates, 833-834
   SMTP notification channels, 832-833
Operations Manager
   global management group settings,
      393-396
   notifications and subscriptions, 399-402
   proxy agent configuration, 396-398
   Restart Health Service Recovery,
      398-399
Operations Manager Dashboard Viewer
   web part, 562
Operations Manager Management Pack,
   433-434
data. See asset data

data flow in Configuration Manager, 101-102
Data Protection Manager. See DPM (Data Protection Manager)
data recovery. See recovery
Data Warehouse Reader accounts, 316
Data Warehouse Write Action accounts, 316
data warehouses
   deploying, 794-797
   explained, 762, 765
   job schedules, viewing, 799-800
Database State view, 482
databases
   audit collection database, 309-310
   backups, 30
   Central Administration Site database, 246
   clusters, 319-320
   CMDB (configuration management database), 765
   design, 686
   Exchange databases
      protecting with DPM (Data Protection Manager), 625-628
      restoring, 628-631
   growth estimates, 93, 326-327
   integrated solutions databases, 22
   Operations Manager database
      backing up, 412-414
      hardware/software requirements, 302
      overview, 301-302
   OperationsManagerAC database, backing up, 416-417
   OperationsManagerDW database, backing up, 414-415
   Orchestration database, 923
   Primary Site Server databases, 246
   replication, 57
   SharePoint content databases, recovering, 649
   Site Database, 246
   Site Server database, 79-81
SQL databases
   choosing versions, 104-105
   preparing for System Center Orchestrator installation, 929
   protecting with DPM, 636-638
   restoring with DPM Recovery Wizard, 638-640
   self-service restores, 640-642
DC Active Alerts, 460
DC events, 460
DC performance data, 460
DC Replication Bandwidth report, 465
DC State, 461
DCM (Desired Configuration Management). See Compliance Settings
Default Management Pack, 456
defining
   collections, 185-188
   management groups, 328-329
defragmentation applications, file exclusions for, 409-410
Delegated Administrator role (VMM), 672, 729, 731-734
delegating guest session administration, 37
deleting
   CI (configuration items), 913-914
   user roles, 740
dependent activities, 886
Deploy Virtual Machine Wizard, 743-744
deploying, 67-68. See also configuring; deployment management; installing
   applications, reports on, 253
certificates, 165
   Configuration Manager clients, 94-95
DPM (Data Protection Manager)
   DPM server, 587
   DPM Setup Wizard, 588-591
   planning for, 580-587
   remote SQL instances, 588
geographic-based management groups, 335
IPs (Integration Packs), 951
operating systems, 11
Operations Manager, 345-346
   design and planning phase, 346-348
   design principles training, 346
   pilot phase, 351-352
   production phase, 352-353
   proof of concept (POC) phase, 348-350
Operations Manager agents, 373
   audit forwarders, 376-379
   UNIX/Linux agents, 379-385
   Windows agents, 373-376
Operations Manager Dashboard Viewer web part, 561-562
political or security-based management groups, 335
protection agents
   with certificates, 599-601
   with DPM Administration Console, 594-596
   manual installation process, 596-599
   with PowerShell, 601
Service Manager
   Active Directory connectors, 805-806
   components, 791-794
   Configuration Manager connectors, 811-812
   data warehouse job schedules, viewing, 799-800
   data warehouses, 794-797
   management group registration, 798-799
   Self-Service Portal, 801-805
   Operations Manager connectors, 806-811
   Orchestrator connectors, 812-813
software, 12
VMM (Virtual Machine Manager)
   multiple-server deployment, 688
   planning for, 682-687
   single-server deployment, 688
   VMM Administrator Console installation, 692-693
   VMM Agent installation, 695-700
   VMM Self-Service Portal installation, 694
   VMM Self-Service Portal security, 695
   VMM server installation, 688-691
VMs (virtual machines) with VMM
   Administrator Console, 742-744
deployment configuration files, 753
deployment management. See also application management
   automatic deployments, 211-213
   best practices, 243-244
   MDT (Microsoft Deployment Toolkit), 238
   creating task sequences, 240-242
   installing, 238
   integrating with Configuration Manager, 239-240
   monitoring deployments, 213-215
   OS deployment. See OS deployment
deployment self-service deployments, 207-211
   targeting users, 203-207

How can we make this index more useful? Email us at indexes@samspublishing.com
update deployment, 219
  automatic deployment rules, creating, 222-224
  deployment packages, creating, 219-220
monitoring, 224-225
Software Update deployments, creating, 220-222
Deployment Manager utility, 923, 950-951
deployment packages, creating, 219-220
Deployment Status of All Task Sequence Deployments report, 254
deployment templates, 221
deployment types, 68
  preparing for OS deployment, 227
design and planning phase
  Operations Manager deployment, 346-348
  Service Manager deployment, 784-786
design principles training (Operations Manager), 346
Design Principles Training phase (Service Manager deployment), 784
design requirements (Service Manager)
  disk subsystem performance, 773
  hardware requirements, 769-771
  large enterprise design, 780-783
  medium enterprise design, 778-780
  SAN versus DAS, 773
  small enterprise design, 776-778
  software requirements, 771-772
  SQL versions, 773-774
design scenarios (Configuration Manager)
  large enterprises, 111-112
  small and medium enterprises, 110-111
designing
collections, 94
Configuration Manager configuration for sample organization, 117
database servers, 686
databases, 686
DPM servers, 586-587
infrastructure fabric, 686-687
library servers, 687
Operations Manager
  large enterprise design, 341-345
  medium enterprise design, 338-341
  small enterprise design, 336-338
  protection groups, 582-585
Self-Service Portal web server, 686
VMM Library, 687
VMM servers, 686
Desired Configuration Management (DCM). See Compliance Settings
DFS namespaces, protecting data in, 621
Diagram view (Operations console), 424
dialog boxes. See names of specific dialog boxes
dip stick health checks (Operations Manager), 403-404
direct attached storage (DAS), 331-333, 773
Disable Audit Collection, 438
disaster recovery (Operations Manager), 320-323
  component backup schedules, 411-412
  IIS 7.x configuration backup, 417-418
  OperationsManager database, 412-414
  OperationsManagerAC database, 416-417
  OperationsManagerDW database, 414-415
discovering
  Configuration Manager clients, 94-95
  sites and subnets, 98-99
discovery methods, configuring, 143-144
Discovery Wizard, 373, 375
Disk Performance Analysis report, 449
Disk Performance Dashboard view, 445
disk subsystem performance, 329-330
  Configuration Manager, 102
  SAN versus DAS, 102-104
  SQL versions, 104-105
  Service Manager, 773
disk-to-disk (D2D) storage, 570
disk-to-disk-to-cloud (D2D2C) storage, 571
disk-to-tape (D2T) storage, 570
disks, adding to storage pool, 591-593
distribution. See content distribution
Distribution Points, 58, 61
  BITS-enabled Distribution Points, 83-84
  BranchCache features, 84
  distributing content to, 202-203
  overview, 82-83
  protected Distribution Points, 84
  PXE-enabled Distribution Points, 97
  selecting, 184-185
  SMB-based Distribution Points, 83
DMZ servers
- certificates, 316
- monitoring with certificates, 385-386
  - agent configuration, 392
  - agent installation, 391-392
  - certificate templates, creating, 386-387
  - root CA server certificates, requesting, 387-390

domain controller discovery, 453
domain controller monitoring scripts, 452

Domain Join account, 91

downloading management packs from Internet, 427-428
Downtime report, 528

DPM (Data Protection Manager), 8
  - advantages over tape-based backup, 569-570
  - best practices, 617-618, 661-662
  - business solutions addressed by, 28
  - CDP (continuous data protection), 571-572
  - custom volumes, 613-614
  - D2D (disk-to-disk) storage, 570
  - D2D2C (disk-to-disk-to cloud) storage, 571
  - D2T (disk-to-tape) storage, 570
  - data recovery, 614-616
  - DPM Administration Console
    - overview, 607-608
    - protection agent deployment, 594-596
  - DPM Central Console, 610-613
  - DPM Management Shell, 608-610
  - DPM servers
    - deploying, 587
    - designing, 586-587
    - preparing for deployment, 587
  - DPM Setup Wizard, 588-591
  - Exchange Server, protecting, 624
    - additional considerations, 635
    - Exchange databases, 625-631
    - high-availability considerations, 633-634
    - mailboxes, 631-633
  - file servers, protecting data, 620-621
    - on DFS namespace, 621
    - on file server clusters, 622
    - on mount points, 622
  - hardware requirements, 578
  - Hyper-V, 654
    - item-level recovery, 659-660
    - protecting Hyper-V virtual machines, 654-656
  - protecting nondomain joined Hyper-V hosts, 656
  - recovering Hyper-V virtual machines, 658-659
  - targeting Hyper-V hosts across firewalls, 656-657
  - major features of, 28-31
  - new features, 32-34
  - overview, 8, 26-27, 567-568
  - planning for, 580
    - DPM servers, 586-587
    - environment, 580-581
    - project scope, 581-582
    - protection groups, 582-585
    - storage requirements, 585
  - ports used by, 657
  - protection agents, deploying
    - with certificates, 599-601
    - with DPM Administration Console, 594-596
    - manual installation process, 596-599
    - with PowerShell, 601
  - protection groups
    - creating, 601-606
    - custom volumes, 613-614
  - remote SQL instances
    - deploying, 588
    - requirements, 579
  - revisions and product history, 31-32
    - Data Protection Manager 2006, 572
    - Data Protection Manager 2006 SP1, 573
    - Data Protection Manager 2007, 573-574
    - Data Protection Manager 2007 SP1, 574-575
    - Data Protection Manager 2010, 575-577
    - Data Protection Manager 2010 SP 1, 575-577
    - Data Protection Manager 2012, 577-578
  - Self Service Recovery Tool, 640-642
  - SharePoint farms
    - content databases, recovering, 649
    - item-level recovery, 650-653
    - preparing for protection, 644-645
    - protecting, 645-647
    - recovering, 647-649
    - SharePoint data sources and recoverable data, 643-644

How can we make this index more useful? Email us at indexes@samspublishing.com
software requirements, 579
SQL Server, 635
  protecting SQL databases, 636-638
  restoring SQL databases with Recovery Wizard, 638-640
  self-service restores, 640-642
storage pool, adding disks to, 591-593
supported operating systems, 579
System State, protecting, 622-624
tape libraries, configuring, 593
dragging and dropping VMs (virtual machines)
o nto host groups, 752
onto host servers, 751-752
driver packages, 70
drivers
  managing, 230-231
  operating system deployment, 70

E
early virtualization management techniques, 673
Edge role, 474
editing
  configuration.mof files, 263-265
  reports (Configuration Manager), 256-261
  SCCM MOF file, 261
email
  email-created incidents, 845
  inbound email settings (Service Manager), 826-830
Email activity (Orchestrator), 953
e-mail subscriptions for reports, configuring, 255
e-mail-created incidents, 845
Enable Audit Collection, 438
enabling. See also configuring
  Internet-based client management, 176-177
  network discovery for Runbook Designer, 939-940
  PXE support, 154-155
  unknown computer support, 234-235
encryption key, backing up, 816-817
Encryption Key Backup or Restore Wizard, 793, 797
end-to-end service monitoring, 292
Endpoint Protection Point section (client settings), 100, 157-158
Endpoint Protection Points, 57-58, 152-153
Enrollment Points, 58
Enterprise Root CA, 109
  deployment, 163-165
  validation, 165
environment
  DPM deployment, 580-581
  VMM deployment, 682-683
  virtualized environments. See Hyper-V
estimating time requirements for Service Manager projects, 791
ETL (Extraction, Transformation, and Loading) process, 767
evaluating incidents, 846-847
event correlation, 20
event logs, 20
Events workspace (Orchestrator console), 948
Exchange 2010 ActiveSync Connectivity view, 473
Exchange 2010 Client Performance report, 478
Exchange 2010 Management Pack, 466
  Correlation Engine service, 467-468
  installing, 468-469
  preparing to install, 466-467
  reports, 477-478
  synthetic transaction event collection, 470-471
  test mailbox configuration, 469-470
  views, 471-477
Exchange 2010 Service State view, 472
Exchange connectors, configuring, 147-148
Exchange databases
  protecting with DPM, 625-628
  restoring, 628-631
Exchange Server
  mailboxes, restoring, 631-633
  protecting with DPM, 624
    additional considerations, 635
  Exchange databases, 625-631
  high-availability considerations, 633-634
    mailboxes, 631-633
Exchange Server connectors, 57
EXE applications, configuring, 192-196
existing user state, capturing, 231
exporting management packs, 429-430
extending Active Directory schema, 118-119
extraction, 767
Extraction, Transformation, and Loading (ETL) process, 767
F

fabric management (VMM), 677, 686
fabric resources, 704
   networks, 706
   servers, 705
   storage, 706-707
failing manual activities, 905-907
fallback sites (Configuration Manager), 57
Fallback Status Point (FSP), 164
   installing, 149
   overview, 84
farms (SharePoint)
   content databases, recovering, 649
   item-level recovery, 645-653
   preparing for protection, 644-645
   protecting with DPM, 645-647
   recovering, 647-649
   SharePoint data sources and recoverable data, 643-644
fault tolerance (Operations Manager)
   architecture, 317
   database clusters, 319-320
   management group redundancy, 318
   resource pools, 318-319
file attachment limits, 887-888
   for incidents, 822
   for problems, 856-857
File Encoding dialog box, 957
File Management activity (Orchestrator), 953
file server clusters, protecting data on, 622
file servers, protecting data with DPM, 620-621
   in DFS namespace, 621
   on file server clusters, 622
   on mount points, 622
files
   deployment configuration files, 753
   exclusions for antivirus and defragmentation applications, 409-410
Filter Settings dialog box, 955, 963
firewalls
   Operations Manager requirements, 314
   System Center Orchestrator, 928
   targeting Hyper-V hosts across, 656-657
Flush Health Service State and Cache, 438
folders, creating for service catalog
   knowledge-base articles, 876
Forensic reports (ACS), 543
forest discovery, configuring, 139
FSP (Fallback Status Point), 164
   installing, 149
   overview, 84
G
Gateway server, 307-308
General License Reconciliation report, 276
General settings (VMM Administrator Console), 715
generating
   Activity Distribution report, 917
   Computer Inventory reports, 919
   Configuration Manager reports, 250-252
generating reports. See schedules, report schedules
geographic views, configuring, 145-147
geographic-based management groups, 335
Get the Agent Processor Utilization, 438
Get the Pool Member Monitoring a Top-Level Instance, 439
Get Top-Level Instances Monitored by a Pool Member, 439
Get User Properties dialog box, 963
Get-Help cmdlet, 716
global management group settings (Operations Manager), 393-396
global roaming, 65, 182
GnuPG (GNU Privacy Guard), 941
group discovery, 95
groups
   host groups
      creating, 708-709
      definition of, 705
management groups
   defining, 328-329
   geographic-based management group, 335
   global management group settings (Operations Manager), 393-396
   multiple management group, 334
   political or security-based management group, 335
   registering, 798-799

How can we make this index more useful? Email us at indexes@samspublishing.com
protection groups
creating, 601-606
custom volumes, 613-614
designing, 582-585
security groups (Orchestrator), 927
software update groups, creating, 216-219
guest sessions, 37-38

Hardware 01A - Summary of Computers in a Specific Collection, 270
Hardware 02A - Estimated Computer Age by Ranges Within a Collection, 270
Hardware 02B - Computers Within an Age Range Within a Collection, 270
Hardware 03A - Primary Computer Users, 270
Hardware 03B - Computers for a Specific Primary Console User, 270
Hardware 04A - Shared (Multi-User) Computers, 271
Hardware 05A - Console Users on a Specific Computer, 271
Hardware 06A - Computers for Which Console Users Could Not Be Determined, 271
Hardware 07A - USB Devices by Manufacturer, 271
Hardware 07B - USB Devices by Manufacturer and Description, 271
Hardware 07C - Computers with a Specific USB Device, 271
Hardware 07D - USB Devices on a Specific Computer, 271
Hardware 08A - Hardware That Is Not Ready for a Software Upgrade, 271
Hardware 09A - Search for Computers, 271
hardware class, adding in client settings, 266
Hardware History node, 269
hardware inventory (Configuration Manager), 59, 71, 261
   adding hardware class in client settings, 266
   creating Registry keys on the client, 261-262
   editing configuration.mof files, 263-265
   manually compiling configuration.mof files on test clients, 265
   validating custom inventory data, 267-268
   viewing custom inventory data, 268

Hardware Inventory Client Agent, 248-249
Hardware Inventory section (client settings), 100, 158

hardware requirements
ACS (Audit Collection Services), 311
Configuration Manager, 92-93
DPM (Data Protection Manager), 578
Gateway server, 307-308
Operations Manager, 323-324
   agents, 301
   audit collection database, 310
   audit collector, 309
   command shell, 307
database, 302
   Operations Console, 305
   Web console, 306
Reporting data warehouse, 303
Reporting Server, 304
Service Manager, 769-771
System Center Orchestrator, 925-926
VMM Administrator Console, 679
VMM Self-Service Portal, 680
VMM server, 678

hash values, 82
Health Service Heartbeat Failure, 433
Health Service Watcher monitors, 433
Health Validator Point, 85
heterogeneous VM management, 670
hierarchy configuration (Configuration Manager), 62-63, 138
   boundaries and boundary groups, 139-143
   changes in, 56-57
   discovery methods, 143-144
   Exchange connectors, 147-148
   hierarchy and geographic views, 145-147
hierarchy views, configuring, 145-147
high-availability considerations
DPM (Data Protection Manager), 633-634
   System Center Orchestrator, 926
holding change requests, 900-903
host clusters, managing, 710
host groups
   creating, 708-709
   definition of, 705
   dragging and dropping VMs onto, 752
host ratings, customizing, 741-742
host servers, dragging and dropping VMs onto, 751-752
hosts
Hyper-V hosts
protecting, 656
targeting across firewalls, 656-657
managing, 709
virtual machine hosts, system
requirements, 682
HTTP client connections, 12
HTTPS
client connections, 12
selecting by roles, 57
Hub Transport role, 474
Hyper-V, 654. See also VMM (Virtual Machine
Manager)
item-level recovery, 659-660
protecting with DPM
protecting Hyper-V virtual machines, 654-656
protecting nondomain joined Hyper-V
hosts, 656
targeting Hyper-V hosts across firewalls, 656-657
recovering Hyper-V virtual machines, 658-659
server backups, 31
VMM support for, 670

I/O Latency, 331
I/Os Per Second (I0ps), 331
IBCM (Internet-based client management), 106-107, 163
Certificate Auto-Enrollment GPO
configuration, 166-168
certificate deployment, 165
certificate requirements, 108-109
Certificate Services website, configuring
for SSL, 174-175
certificate templates, 109-110
creating, 168-172
publishing, 172-173
client site assignment, 108
content distribution, 184
enabling, 176-177
Enterprise Root CA, 163-165
limitations of, 107
OS Deployment certificate requests, 176
PKI creation, 163
planning PKI, 109
planning site system placement, 107-108
task sequence deployment, 59
WSUS website, configuring for SSL,
175-176
IBM AIX 5.3 dependencies, 379
IBM AIX 6.1 dependencies, 380
IDMIF files, asset data, 247
IIS
configuration backup, 417-418
implementing on Site Servers, 121-124
ILR (item-level recovery)
on Hyper-V virtual machines, 659-660
of SharePoint items, 650-653
implementing change requests, 903
approving and rejecting review activities, 903-905
automatic user notification, 908-910
closing, 907-908
completing and failing manual activities, 905-907
importing
application packages into VMM, 758
management packs, 365-368, 426-427
software license data, 275-277
unknown computers, 234-235
inbound email settings (Service Manager), 826-830
incident management, 42
incidents
analyzing, 847-849
announcements, publishing, 850
assigning, 846-847
e-mail-created incidents, 845
evaluating, 846-847
explained, 819-820
closed, 821-822
incident reports, 864-868
incident settings
file attachment limits, 822
inbound email settings, 826-830
incident prefix, 821
Operations Manager Web console
settings, 826
priority calculation, 822-824
resolution times, 824-825
How can we make this index more useful? Email us at indexes@samspublishing.com
manually created incidents, 836-838
Operations Manager alert-generated incidents, 838-841
resolving, 853-855
Self-Service Portal-generated incidents, 841-845
troubleshooting tasks, running, 851-853
infrastructure fabric design, 686-687
infrastructure optimization model (Service Manager 2012), 871-872
initiating change requests, 892-893
installation prerequisites (Configuration Manager), 118
adding Windows roles on Site Servers, 121-124
configuring System Management container, 120-121
extending Active Directory schema, 118-119
Installation Summary screen (Orchestrator Setup Wizard), 932
installing. See also deploying
agents on DMZ servers, 391-392
Asset Intelligence Synchronization Point role, 153-154
Central Administration Site, 124-129
clients (Configuration Manager), installation settings, 162-163
complex applications, automating installation, 197-198
Endpoint Protection Point role, 152-153
Exchange 2010 Management Pack, 468-469
FSP (Fallback Status Point), 149
IPs (Integration Packs), 949, 951
management packs from downloads, 429
MDT (Microsoft Deployment Toolkit), 238
Operations Manager, 356
ACS (Audit Collection Services), 368-373
management packs, importing, 365-368
multiserver installs, 359-365
single-server installs, 356-359
Primary Site Servers, 129-133
RSP (Reporting Service Point), 149-150
secondary sites, 134-138
Server App-V Agent, 754-755
Server App-V Sequencer, 754
Service Manager
Active Directory connectors, 805-806
components, 791-794
Configuration Manager connectors, 811-812
data warehouse job schedules, viewing, 799-800
data warehouses, 794-797
management group registration, 798-799
Self-Service Portal, 801-805
Operations Manager connectors, 806-811
Orchestrator connectors, 812-813
Software Update Point role, 150-152
State Migration Point, 155
System Center Orchestrator
multiserver installation, 933-939
single-server installation, 928-932
UNIX/Linux agents, 379-385
VMM Administrator Console, 692-693
VMM Agent, 695-700
VMM Self-Service Portal, 694
VMM servers, 688-691
Windows agents, 373-376
instances (VMM), number of, 685
Instances tab
   Runbook Servers workspace, 948
   Runbooks workspace, 947
integrated solutions databases, 22
integrating MDT 2012 with Configuration Manager 2012, 239-240
Integration Pack Deployment Wizard, 951
Integration Packs. See IPs (Integration Packs)
Integration Toolkit (Orchestrator), 923
Internet-based client management. See IBCM
Internet-based Management Points, 58
inventory collection, 71
   asset data, 246-247
   configuring client settings, 248-249
inventory data
   validating, 267-268
   viewing, 268
inventory reports, 252
investigating change requests, 896-898
IOps (I/Os Per Second), 331
IPs (Integration Packs)
   deploying, 951
   explained, 923
   installing, 949, 951
   registering, 950-951
ISO 20000 international standard, 885
IT Process Automation (ITPA), 765
Item Selection dialog box, 963
item-level recovery (ILR)
on Hyper-V virtual machines, 659-660
of SharePoint items, 650-653
items (SharePoint), recovering, 650-653
ITIL Change Management, 885
ITIL Service Management, 885
ITPA (IT Process Automation), 765

J–K
job schedules, viewing, 799-800
Jobs dialog box, 714
Jobs tab
Runbook Servers workspace, 948
Runbooks workspace, 947
Junction Properties dialog box, 958
Kerberos tickets, refreshing, 91, 120, 171
keys, backing up encryption key, 816-817
knowledge base (KB), 765, 768
creating folders for articles, 876

L
large enterprise design
Configuration Manager, 111-112
Operations Manager, 341-345
Service Manager, 780-783
latency, 331
libraries
tape libraries, configuring, 593
VMM Library
configuring, 710-711
designing, 687
explained, 668-669
library servers, 687, 705
License 01A - Microsoft License Ledger for
Microsoft License Statements, 271
License 01B - Microsoft License Ledger Item by
Sales Channel, 272
License 01C - Computers with a Specific
Microsoft License Ledger Item and Sales
Channel, 272
License 01D - Microsoft License Ledger
Products on a Specific Computer, 272
License 02A - Count of Licenses Nearing
Expiration by Time Ranges, 272
License 02B - Computers with Licenses Nearing
Expiration, 272
License 02C - License Information on a Specific
Computer, 272
License 03A - Count of Licenses by License
Status, 272
License 03B - Computers with a Specific
License Status, 272
License 04A - Count of Products Managed by
Software Licensing, 272
License 04B - Computers with a Specific
Product Managed by Software Licensing
Service, 273
License 05A - Computers Providing Key
Management Service, 273
license data, importing, 275, 277
licensing, 6, 50
core client access licenses, 50
costs, SQL, 105
server management suite volume licensing,
50-51
tracking, 72
limits on file attachments, 887-888
Linux agents, installing, 379-385
List of Activities report, 917
List of Change Requests report, 916
List of Manual Activities report, 917
List of Review Activities report, 917
listings
Customizing the configuration.mof File, 264
PowerShell Script to Check the Hardware
Warranty Status, 279
Query for Count Operating Systems and
Service Packs Report, 259
Query for Listing Systems with Operating
Systems and Service Packs, 259
VBScript to Check the Hardware Warranty
Status, 280
lists
Configuration Manager reports, 252-255
SharePoint lists, recovering, 650-653
load balancers, 706
loading, 767
Local Administrator accounts, 316

How can we make this index more useful? Email us at indexes@samspublishing.com
Local Agent Compliance report, 285
Local Service account, 91
Local System account, 91
Log pane (Runbook Designer), 945
Logical Disk Free Space monitor, 441
logical networks, 706
logs, event, 20

M
MAC address pools, 706
Machine Level Capacity Trending report, 477
Mailbox role, 475
mailboxes, restoring, 631-633
Maintenance mode (VMM 2008 R2), 675-676
maintenance reports (Operations Manager), 532
    Alert Logging Latency report, 534-536
    Daily Alerts report, 538-540
    Most Common Alerts report, 533-534
    Send Queue % Used Top 10 report, 536-537
    SQL Database Space report, 540-541
maintenance windows for collections, 187
managed systems, 62
Management 2 - Updates Required but Not Deployed report, 253
management console (Configuration Manager), role-based administration, 89
management groups
defining, 328-329
geographic-based management groups, 335
global management group settings (Operations Manager), 393-396
multiple management groups, 334
political or security-based management groups, 335
redundancy, 318
registering, 798-799
Management Pack Import Wizard, 367-368
Management Pack Templates, 491-492
    OLEDB Data Source Template, 497-499
    Process Monitoring Template, 499-500
    TCP Port Template, 501-502
    UNIX/Linux Log File Template, 502
    UNIX/Linux Service Template, 503
    Web Application Template, 492-494
    Windows Service Template, 494-497
management packs, 291. See also names of specific management packs
    importing, 365-368, 426-427
    updating, 404-405
Management Point (MP), 58, 61, 246
    overview, 85-86
    secondary sites and, 64
    server locator functionality, 58
management server (Orchestrator), 923
    connecting to Runbook Designer, 940-941
    installing, 934-935
Management Server Action accounts, 315
Management Server State Dashboard view, 437
Management Server to Management Group Availability Health Rollup, 433
management servers, 300-301
Management Servers State, 436
Management Shell (DPM), 608-610
managing. See also administration
    Administrator user role, 730-731
    host clusters, 710
    hosts, 709
    Hyper-V with VMM. See VMM (Virtual Machine Manager)
    VMs (virtual machines), 714
manual activities, 886, 898
    adding to change requests, 897
    completing, 905-907
    failing, 905-907
Manual Activity Details report, 917
manually created incidents, 836-838
MBps (Megabytes Per Second), 331
MDT (Microsoft Deployment Toolkit), 70, 238
    creating task sequences, 240-242
    installing, 238
    integrating with Configuration Manager, 239-240
medium enterprise design
    Configuration Manager, 110-111
    Operations Manager, 338-341
    Service Manager, 778-780
Megabytes Per Second (MBps), 331
Message Properties dialog box, 957
Microsoft Deployment Toolkit. See MDT
    (Microsoft Deployment Toolkit)
Microsoft Installer, 189
Microsoft Operations Manager (MOM) 23
Microsoft Software License Terms dialog box, 589
Microsoft Solution Accelerators, 9
Microsoft System Center Enterprise Suite Unleashed, 9
Migrate action (VMM), 748-750
Migrate Storage action (VMM), 750-751
Migrate Virtual Machine Wizard
  Migrate action, 748-750
  Migrate Storage action, 750-751
migrating VMs (virtual machines)
  dragging and dropping onto host group, 752
  dragging and dropping onto host server, 751-752
  with Migrate action, 748-750
  with Migrate Storage action, 750-751
  supported storage migration technologies, 748
  supported VM migration technologies, 747-748
Mobile Device Management, 9, 87-88
Mobile Device section (client settings), 100
Modify Disk Allocation dialog box, 614
modifying
  existing XML management pack, 506
  stored procedures, 450
  user roles, 739-740
mofcomp.exe utility, 263
MOF files (Configuration Manager), editing, 261
MOM (Microsoft Operations Manager), 23
Monitor Availability report, 528
Monitor File Properties dialog box, 955
monitoring
  applications, 21, 290
  baselines and compliance, 283
  clients, 20-21
  deployments, 213-215
  DMZ servers, 385-386
    agent configuration, 392
    agent installation, 391-392
    certificate templates, creating, 386-387
    root CA server certificates, requesting, 387-390
  networks, 290, 385
  non-domain member considerations, 327-328
  OS deployment, 236-238
  rules, 294
  servers, 20
  system monitoring, 21
  update deployment, 224-225
  VMs (virtual machines), 714
Monitoring activity (Orchestrator), 953
Monitors, 292
Most Common Alerts report, 533-534
mount points, protecting data on, 622
Move Disabled Users runbook
  building, 962-965
  testing, 965-966
Move User Properties dialog box, 963
MSI applications, configuring, 191-192
MSI extension, 189
multiple Internet-based Management Points, 58
multiple management groups, 334
multiple-server deployment (VMM), 688
multiserver installations
  Operations Manager, 359-365
  Orchestrator, 933
    hardware requirements, 925-926
    management server installation, 934-935
    Orchestrator web service installation, 937-938
    Runbook Designer installation, 938-939
    runbook server installation, 935-937
    server preparation, 933
multisite hierarchy in Configuration Manager, 95-96

N

namespaces, protecting data in, 621
Native mode, 57
NetIQ Enterprise Event Manager, 23
Network Access account, 91, 95, 227
Network Access Protection section (client settings), 100
Network Discovery, 95, 939-940
networks
  logical networks, 706
  monitoring, 290, 385
  Operations Manager requirements, 325-326
  SANs (storage area networks), 331-333
  VMM private cloud, 706

How can we make this index more useful? Email us at indexes@samspublishing.com
new features
Configuration Manager, 15-17, 56-60
DPM (Data Protection Manager), 32-34
Operations Manager, 24-25, 290-291
Service Manager, 44-45, 762-763
System Center 2012 Orchestrator, 48-49
VMM (Virtual Machine Manager), 39, 677-678
New Job Schedule dialog box, 413-417, 815-816
NOIDMIF files, 247
nondomain joined Hyper-V hosts, protecting, 656
Notification activity (Orchestrator), 953
notifications
alert tuning, 405-409
configuring, 399-402
definition of, 293
Notifications Resource Pool, 319
Service Manager notifications, 830
architecture, 830-832
notification subscriptions, 834-835
notification templates, 833-834
SMTP notification channels, 832-833
Notifications Resource Pool, 319

Office Customization Wizard, 197-198
OLAP cubes, 768-769
OLEDB Data Source Template, 497-499
Opalis, 48
operating system deployment. See OS deployment
Operating System Health Dashboard view, 444
operating system images, managing, 229-230
operating system install package, 70
operating system install task sequences, creating, 231-234
operating system installers, managing, 228-229
Operating System Performance view, 444
operating system source files, 69
operating systems, support for
in DPM (Data Protection Manager), 579
in Operations Manager, 298
in System Center Orchestrator, 924-925
in VMM (Virtual Machine Manager), 679-681

Operations console, 304-305, 422-424
Operations Manager, 18, 421
ACS (Audit Collection Services)
hardware/software requirements, 311
installing, 368-373
overview, 310-311
agents, 373
audit forwarders, configuring, 376-379
configuring to use certificates, 392
installing on DMZ servers, 391-392
overview, 298-299
proxy agent configuration, 396-398
Restart Health Service Recovery, 398-399
security, 313
supported operating systems, 298
UNIX/Linux agents, installing, 379-385
Windows agents, installing, 373-376
alerts
generating, 294
overview, 292
tuning, 405-409
architecture, 296-298
audit collection database, 309-310
audit collector, 309
audit forwarder
configuring, 376-379
overview, 308
backups
component backup schedules, 411-412
IIS 7.x configuration backup, 417-418
OperationsManager database, 412-414
OperationsManagerAC database, 416-417
OperationsManagerDW database, 414-415
best practices, 354, 418-419, 566
business solutions addressed by, 19-20
command shell, 306-307
connectors, deploying, 806-811
dashboards
creating, 557-559
explained, 554-555
publishing, 561-565
viewing, 559-560
widgets, 556-559
data storage, 329
database sizing, 326-327
deploying, 345-346
design and planning phase, 346-348
design principles training, 346
pilot phase, 351-352
production phase, 352-353
proof of concept (POC) phase, 348-350
time estimates, 353
design
- large enterprise design, 341-345
- medium enterprise design, 338-341
- small enterprise design, 336-338
dip stick health checks, 403-404
disaster recovery, 320-323
disk subsystem performance, 329-330
DMZ servers, monitoring with certificates, 385-386
- agent configuration, 392
- agent installation, 391-392
- certificate templates, creating, 386-387
- root CA server certificates, requesting, 387-390
fault tolerance
- architecture, 317
- database clusters, 319-320
- management group redundancy, 318
- resource pools, 318-319
file exclusions for antivirus and defragmentation applications, 409-410
Gateway server, 307-308
global management group settings, 393-396
hardware requirements, 323-324
how it works, 291, 293
installing, 356
- ACS (Audit Collection Services), 368-373
- management packs, importing, 365-368
- multiserver installs, 359-365
- single-server installs, 356-359
integrating with VMM deployment, 684
major features, 20-23
management groups
- defining, 328-329
- geographic-based management group, 335
- multiple management group, 334
- political or security-based management group, 335
management packs, 291, 425-426
- downloading from Internet, 427-428
- exporting, 429-430
- importing from Internet, 426-427
- manually installing from downloads, 429
- overrides, 430-432
- updating, 404-405
management servers, 300-301
monitoring rules, 294
monitors, 292
network bandwidth requirements, 325-326
network monitoring, 385
new features, 24-25, 290-291
non-domain member considerations, 327-328
notifications
- alert tuning, 405-409
- configuring, 399-402
Operations console, 304-305, 422-424
Operations Manager database, 301-302
overview, 8, 19
Reporting data warehouse, 302-303
Reporting Server, 304
reports, 295-296
- Alert Logging Latency report, 534-536
- Alerts reports, 525-527
- Availability reports, 527-531
- charts, displaying, 531-532
- explained, 512-513
- Most Common Alerts report, 533-534
- Performance By System reports, 523-524
- Performance By Utilization reports, 523-524
- Performance reports, 514-520
- Performance Top Instances reports, 520-522
- Performance Top Objects reports, 520-522
- Send Queue % Used Top 10 report, 536-537
- Service Level Tracking reports, 551-554
- SLAs (service-level agreements), 548-549
- SLOs (Service Level Objectives), 549-551
responses, generating, 294
revisions and product history, 23-24

How can we make this index more useful? Email us at indexes@samspublishing.com
rules, 292
SAN versus DAS, 331-333
security
- Action accounts, 315-316
- agents, 313
- certificates, 316
- firewalls, 314
- role-based security model, 311-313
- RunAs accounts, 316
SLT (Service Level Tracking), 293
software requirements, 324
SQL Server versions, 333-334
subscriptions, configuring, 399-402
Web console, 424-425
- hardware/software requirements, 306
- overview, 305-306
- Performance view time frame, 410-411
Operations Manager alert–generated incidents, 838-841
Operations Manager Dashboard Viewer web part
- adding to SharePoint page, 562-565
- configuring, 562
- deploying, 561-562
Operations Manager Management Pack, 421, 432-433
- configuring, 433-434
- tasks, 438-439
- views, 434-437
Operations Manager Web console settings
- (Service Manager), 826
OperationsManager database, backing up, 412-414
OperationsManagerAC database, backing up, 416-417
OperationsManagerDW database, backing up, 414-415
Operator role (Operations Manager), 312
OpsMgr. See Operations Manager
OpsMgrLatencyMonitors container, 457
Orchestration console, 923, 946-948
Orchestration database, 923
Orchestration Integration Toolkit, 923
Orchestrator
- best practices, 968
- business solutions addressed by, 46-47, 922
- connectors, deploying, 812-813
Deployment Manager, 923
- hardware requirements, 925-926
- high-availability considerations, 926
IPs (Integration Packs)
- deploying, 951
- explained, 923
- installing, 949, 951
- registering, 950-951
major features of, 47-48
management server, 923
- connecting to Runbook Designer, 940-941
- installing, 934-935
multiserver installation, 933
- management server installation, 934-935
- Orchestration web service installation, 937-938
- Runbook Designer installation, 938-939
- runbook server installation, 935-937
- server preparation, 933
new features, 48-49
Orchestration console, 923, 946-948
Orchestration database, 923
Orchestration Integration Toolkit, 923
Orchestrator web service, 923
- installing, 937-938
- overview, 9, 45, 921-922
postinstallation tasks
- connecting Runbook Designer to management server, 940-941
- enabling GNU Privacy Guard, 941
- enabling network discovery for Runbook Designer, 939-940
product history, 48
revisions and product history, 924
Runbook Designer, 923
- Activities pane, 945
- connecting to Active Directory, 952
- connecting to management server, 940-941
- Connections pane, 943-944
- enabling network discovery for, 939-940
- GNU Privacy Guard, 941
- installing, 938-939
- Log pane, 945
- main screen, 942
- workspace, 944-945
runbook server, 923
  installing, 935-937
runbook tester, 923
runbooks
  Copy File and Log Event runbook, 953-961
  Move Disabled Users runbook, 962-966
permissions, 967
standard activities, 952-953
security
  firewall requirements, 928
service accounts, 926-927
single-server installation, 928
  Orchestrator Setup Wizard, 929-932
server preparation, 929
SQL database preparation, 929
supported operating systems, 924-925
Orchestrator Setup Wizard, 929-932
  management server installation, 934-935
Orchestrator web service installation, 937-938
Runbook Designer installation, 938-939
runbook server installation, 935-937
Orchestrator web service, 923
  installing, 937-938
OS deployment, 11, 69-70, 225-227
  application and deployment type preparation, 227
  boot image management, 231
driver management, 230-231
  importing unknown computers, 234-235
  monitoring, 236-238
  operating system image management, 229-230
  operating system install task sequences, creating, 231-234
  operating system installer management, 228-229
preparing for, 154-155
  scenarios for, 226-227
task sequence deployment, creating, 235-236
technologies for, 225-226
  User State Migration package, creating, 227-228
OS Deployment certificate requests, 176
OS Deployment certificate template, creating, 170
OSCapture Account, 91
Out-of-Band Service Points, 86
overlapping boundaries, 98
Override Properties dialog box, 432, 613
overrides, management packs, 430-432
Overides nodes, 432

P

P2V (physical-to-virtual) conversions, 36, 717-724
package model (application management), 190-191
packages, 67
  User State Migration package, creating, 227-228
  virtual application packages
    creating, 755-758
    definition of, 753
    importing into VMM, 758
parallel activities, 886
patch management. See software update distribution; update management
patches, 11
  Performance by System report, 449, 523-524
  Performance by Utilization report, 449-450, 523-524
  Performance Counter View Raw report, 477
  Performance Counter View report, 477
  Performance Data view, 436
  performance in Configuration Manager, 102
    SAN versus DAS, 102-104
    SQL versions, 104-105
  Performance Nutrition report, 477
  Performance reports (Operations Manager), 514-520
  Performance Top Instances reports (Operations Manager), 520-522
  Performance Top Objects reports (Operations Manager), 520-522
  Performance view (Web console), 410-411
performance widgets
  adding to dashboards, 558-559
  explained, 556

How can we make this index more useful? Email us at indexes@samspublishing.com
permissions
Operations console, 424
runbook permissions, 967
Permissions dialog box, 967
physical-to-virtual (P2V) conversions, 36, 717-724
Pilot phase
Operations Manager deployment, 351-352
Service Manager deployment, 789-790
Ping Computer (with Route), 439
Ping Computer Continuously (ping —t), 439
PKI (Public Key Infrastructure)
creating, 163
planning, 109
placement of VMs (virtual machines), 740-741
planning
Configuration Manager client settings, 99-101
DPM (Data Protection Manager)
deployment, 580
DPM servers, 586-587
environment, 580-581
project scope, 581-582
protection groups, 582-585
storage requirements, 585
Operations Manager deployment, 345-346
design and planning phase, 346-348
design principles training, 346
pilot phase, 351-352
production phase, 352-353
POC (Proof of Concept) phase, 348-350
time estimates, 353
Service Manager deployment, 783-784
Design and Planning phase, 784-786
Design Principles Training phase, 784
Pilot phase, 789-790
POC (Proof of Concept) phase, 786-788
Production phase, 790
time estimates, 791
VMM (Virtual Machine Manager)
deployment, 682
database server and database
design, 686
environment, 682-683
infrastructure fabric, 686-687
library server and library design, 687
Operations Manager integration, 684
project scope, 683-684
Self-Service Portal web server
design, 686
VMM instances, 685
VMM server design, 686
planning details, adding to change
requests, 898
Planning reports (ACS), 543
POC (Proof of Concept) phase
Operations Manager deployment, 348-350
Service Manager deployment, 786-788
policies, explained, 62
Policy reports (ACS), 543
political-based management groups, 335
pool tasks, 439
port groups for virtual switches, 676
port requirements in Configuration Manager,
89-90
portals, support for, 44
ports, DPM (Data Protection Manager), 657
postinstallation tasks (Orchestrator)
connecting Runbook Designer to
management server, 940-941
enabling GNU Privacy Guard, 941
enabling network discovery for Runbook
Designer, 939-940
PowerShell. See Windows PowerShell
Preboot Execution Environment. See PXE
prefixes
for incidents, 821
problem prefixes, 856
preparing
applications and deployment types for
OS deployment, 227
SharePoint for protection, 644-645
Prerequisite Checker tool, 60, 125
prerequisites, Configuration Manager
installation, 118
adding Windows roles on Site Servers,
121-124
configuring System Management container,
120-121
extending Active Directory schema, 118-119
primary computers, designating, 205-207
Primary Site Server databases, 246
Primary Site Servers
Central Administration Site, 124
installing, 124-126
validating installation, 127-129
installing, 129-133
overview, 78
primary sites (Configuration Manager), 57
primary systems, targeting deployments to, 200-202
priority
of incidents, 822-824
of problems, 857-858
private clouds
creating, 711-714
explained, 704
fabric resources, 704
networks, 706
servers, 705
storage, 706-707
problem prefix strings, customizing, 856
problems. See also troubleshooting
analyzing, 860-861
creating change requests, 895
explained, 819-821
problem records, creating, 859-860
problem reports, 869
resolving, 862-863
settings
file attachment limits, 856-857
priority calculation, 857-858
problem prefix string, 856
Process Management Packs, 764
Process Monitoring Template, 499-500
process validation, 48
processes, service management, 764-765
Production phase
Operations Manager deployment, 352-353
Service Manager deployment, 790
profiles. See roles
programs, 67
Progress of All Task Sequences report, 254
project scope. See scope
Proof of Concept (POC) phase
Operations Manager deployment, 348-350
Service Manager deployment, 786-788
protected Distribution Points, 84
protecting data. See DPM (Data Protection Manager)
Protection Agent Installation Wizard, 595-596
protection agents, deploying
with certificates, 599-601
with DPM Administration Console, 594-596
manual installation process, 596-599
with PowerShell, 601
protection groups
creating, 601-606
custom volumes, 613-614
designing, 582-585
Protocol Downtime Details report, 477
proxy agents, configuring, 396-398
Public Key Infrastructure (PKI)
creating, 163
planning, 109
Published Data dialog box, 956-957, 959
publishing
announcements, 850
certificate templates, 172-173
CRL, 165
Operations Manager dashboards, 561
adding web part to SharePoint page, 562-565
configuring web part, 562
deploying web part, 561-562
pushing agents, 59
PXE servers, 705
PXE support, enabling, 154-155
PXE Server Points, 58
PXE-enabled Distribution Points, 58, 83, 97

Q–R
RAID, 103, 332-333
RAs (review activities), 886, 903-905
Read-Only Administrator role (VMM)
creating, 734-735
explained, 730
Read-Only Operator role (Operations Manager), 312
reboots, suppressing, 227
Recipient Properties dialog box, 964
records, creating problem records, 859-860
recovery
Configuration Manager options, 60
content databases, 649
with DPM (Data Protection Manager), 614-616
Hyper-V item-level recovery, 659-660
Hyper-V virtual machines, 658-659
modern data recovery needs, 568-569

How can we make this index more useful? Email us at indexes@samspublishing.com
Operations Manager, 320-323
Restart Health Service Recovery, enabling, 398-399
SharePoint farms, 647-649
SharePoint sites, lists, and items, 650-653
tape-based solutions, limitations of, 569-570
Recovery Wizard, 638-640
Exchange databases, 629-631
Exchange mailboxes, 632-633
Hyper-V virtual machines, 659
SharePoint farms, 648
SQL databases, 639-640
refreshing Kerberos tickets, 91, 120, 171
regional roaming, 65, 182
registering
   IPs (Integration Packs), 950-951
   Service Manager management groups, 798-799
Registry keys, creating on clients, 261-262
rejecting RAs (review activities), 903-905
release management (Service Manager), 882-884
Reload Configuration, 439
Remote Control - All Computers Remote
   Controlled by a Specific User report, 255
remote control (Control+Alt+Delete), 59
remote control (Configuration Manager), 12
Remote Data Access Service Check
   monitor, 434
Remote Desktop, 439
Remote Desktop (Admin), 439
Remote Desktop (Console), 439
Remote PowerShell Service report, 477
remote SQL instances, DPM deployment, 588
Remote Tools section (client settings), 100, 158-159
removing. See deleting
replication latency, 120
Report Builder report, 258
Report Operator role (Operations Manager), 312
Report Security Administrator role (Operations Manager), 312
reporting, 249
   AI (Asset Intelligence), 277
   software metering data, 278
   VMs (virtual machines), 714
reporting classes, AI (Asset Intelligence), 270-274
Reporting data warehouse, 302-303
Reporting Points, 58
Reporting Server, 304
Reporting Service Point (RSP)
   installing, 149-150
   overview, 87
Reporting Services, 255
   reports, 12, 23, 914
   ACS (Audit Collection Services) reports
      Access Violation reports, 542
      Account Management reports, 542-543
      custom reports, 545-548
      explained, 541-542
      Forensic reports, 543
      generating, 544-545
      overview, 310-311
      Planning reports, 543
      Policy reports, 543
      System Integrity reports, 543
      Usage reports, 544
   Active Directory Management Pack, 465-466
   activity management reports, 917-918
   change management reports, 915-917
   configuration management reports, 918-919
   Configuration Manager reports, 74-75
      editing, 256-261
      generating, 250-252
      lists of, 252-255
      scheduling, 255-256
   configuring email subscriptions for, 255
   consolidated reporting, 43
   Cross Platform Management Packs, 489-490
   Exchange 2010 Management Pack, 477-478
   Operations Manager reports, 295-296
      Alert Logging Latency report, 534-536
      Alerts reports, 525-527
      Availability reports, 527-531
      charts, displaying, 531-532
      Daily Alerts report, 538-540
      explained, 512-513
      Most Common Alerts report, 533-534
      Performance By System reports, 523-524
Performance By Utilization reports, 523-524
Performance reports, 514-520
Performance Top Instances reports, 520-522
Performance Top Objects reports, 520-522
Send Queue % Used Top 10 report, 536-537
Service Level Tracking reports, 551-554
SQL Database Space report, 540-541
Report Builder report, 258
Service Manager reports, 863
incident reports, 864-868
problem reports, 869
report controls, 863-864, 915
SLA (service-level agreement) reporting, 23
SQL Server Management Pack, 486-487
Windows Management Pack, 448-451
Request offerings (Service Manager 2012), 873
creating, 877-879
submitting with Self-Service Web Portal, 880-881
requesting
OS Deployment certificates, 176
root CA server certificates, 387-390
requirements. See hardware requirements; prerequisites; software requirements; system requirements
resetting status summarizer, 128, 133
resolution times for incidents, 824-825
resolving
incidents, 853-855
problems, 862-863
resource pools, 290, 318-319
responses, generating, 294
Restart Health Service Recovery, enabling, 398-399
restoring
CI (configuration items), 914
Exchange databases, 628-631
mailboxes, 631-633
SQL Server databases
with DPM Recovery Wizard, 638-640
self-service restores, 640-642
Resume Health Service recovery, 433
resuming change requests, 900-903
Return to Activity change requests, 902
review activities (RAs), 886, 903-905
Review Activity Details report, 917
reviewers, adding to change requests, 898-899
roaming, 62
client roaming, 65-66, 182-183
global versus regional roaming, 65, 182
role Level Capacity Trending, 477
role-based administration (Configuration Manager), 60
role-based security, 89, 311-313
roles
explained, 61
selecting HTTPS by, 57
VMM user roles, 672-673, 729
Administrator, 729-731
Delegated Administrator, 729, 732-734
modifying, 739-740
Read-Only Administrator, 730, 734-735
removing, 740
Self-Service User, 730, 735-739
Root CA server certificates, requesting, 387-390
RSP (Reporting Service Point)
installing, 149-150
overview, 87
Rule node, 442
rules, 292-294
RunAs accounts, 316
runbook automation, 765, 886
Runbook Control activity (Orchestrator), 953
Runbook Designer, 923
Activities pane, 945
connecting to Active Directory, 952
connecting to management server, 940-941
Connections pane, 943-944
enabling network discovery for, 939-940
GNU Privacy Guard, 941
installing, 938-939
Log pane, 945
main screen, 942
workspace, 944-945
runbook server (Orchestrator), 923
installing, 935-937
Runbook Servers workspace (Orchestration console), 948
runtime tester (Orchestrator), 923

How can we make this index more useful? Email us at indexes@samspublishing.com
runbooks
Copy File and Log Event runbook
building, 953-959
testing, 959-961
creating, 47
definition of, 764
Move Disabled Users runbook
building, 962-965
testing, 965-966
permissions, 967
runbook automation, 765
standard activities, 952-953
testing, 47
Runbooks tab (Runbooks workspace), 947
Runbooks workspace (Orchestration console), 947
running troubleshooting tasks, 851-853

S
Sanbolic Clustered File System (CFS), 676
SANs (storage area networks), 331-333, 773
  DAS (direct attached storage) versus, 102-104
  VMM support for transfers, 676
Scan 1 - Last Scan States by Collection report, 253
SCCM (System Center Configuration Manager).
  See Configuration Manager
schedules
  client schedules, 105-106
  report schedules
    ACS (Audit Collection Services) reports, 541-548
    Alert Logging Latency report, 534-536
    Alerts reports, 525-527
    Availability reports, 527-531
    Configuration Manager, 255-256
    Daily Alerts report, 538-540
    Most Common Alerts report, 533-534
    Performance By System reports, 523-524
    Performance By Utilization reports, 523-524
    Performance reports, 514-520
    Performance Top Instances reports, 520-522
    Performance Top Objects reports, 520-522
    Send Queue % Used Top 10 report, 536-537
    Service Level Tracking reports, 551-554
    SQL Database Space report, 540-541
    Runbook Designer schedules, 944
Scheduling activity (Orchestrator), 953
schema (AD) extensions, 64-66
SCOM (System Center Operations Manager).
  See Operations Manager
scope
    DPM deployment, 581-582
    VMM deployment, 683-684
SCSM (System Center Service Manager). See Service Manager
SDK and Configuration service accounts, 315
sealing management packs via command line, 507
searching CI, 911-912
secondary sites (Configuration Manager), 57
  installing, 134-138
  Management Points and, 64
security. See also DPM (Data Protection Manager)
  certificates. See certificates
    Configuration Manager, 88
      port requirements, 89-90
      role-based administration, 89
      server communication, 88-89
      service accounts, 91
    Distribution Points, 82
    Exchange Server, 624
      additional considerations, 635
      Exchange databases, 625-631
      high-availability considerations, 633-634
      mailboxes, 631-633
    file servers, protecting with DPM (Data Protection Manager), 620-621
      data in DFS namespace, 621
      on file server clusters, 622
      on mount points, 622
    Hyper-V, 654
      item-level recovery, 659-660
      protecting Hyper-V virtual machines, 654-656
      protecting nondomain joined Hyper-V hosts, 656
      recovering Hyper-V virtual machines, 658-659
targeting Hyper-V hosts across firewalls, 656-657
Operations Manager
  Action accounts, 315-316
  agents, 313
  certificates, 316
  firewalls, 314
  role-based security model, 311-313
  RunAs accounts, 316
  runbook permissions, 967
SharePoint farms
  content databases, recovering, 649
  item-level recovery, 650-653
  preparing for protection, 644-645
  protecting with DPM, 645-647
  recovering, 647-649
  SharePoint data sources and recoverable data, 643-644
SQL Server, 635
  protecting with DPM, 636-638
  restoring with DPM Recovery Wizard, 638-640
  self-service restores, 640-642
System Center Orchestrator
  firewall requirements, 928
  security groups, 927
  service accounts, 926-927
  System State, protecting, 622-624
  VMM Self-Service Portal, 695
security groups (Orchestrator), 927
security roles, 89
security scopes, 89
Security settings (VMM Administrator Console), 715
security-based management groups, 335
Select Backup Destination dialog box, 412-417, 815
Select Features to Install screen (Orchestrator Setup Wizard), 930
Select Host page
  Convert Physical Server Wizard, 721
  Convert Virtual Machine Wizard, 727
Select Networks page
  Convert Physical Server Wizard, 723
  Convert Virtual Machine Wizard, 728
Select Path page
  Convert Physical Server Wizard, 723
  Convert Virtual Machine Wizard, 727
Select Source page (Convert Physical Server Wizard), 719
Select the Installation Location screen (Orchestrator Setup Wizard), 932
Select Virtual Machine Source dialog box, 726
  selecting
    Distribution Points, 184-185
    SQL versions, 773-774
Self Service Recovery Tool (DPM), 640-642
self-service creation of guest sessions, 37
self-service deployments, 207-211
Self-Service Portal (VMM)
  creating VMs with, 745-747
  deploying, 801-805
  explained, 668, 763, 765
  hardware requirements, 680
  installing, 694
  security, 695
  software requirements, 681
  supported operating systems, 681
self-service restores of SQL databases, 640-642
Self-Service User role (VMM), 673
  creating, 735-739
  explained, 730
  modifying, 739-740
  removing, 740
Self-Service Web Portal
  creating incidents with, 841-845
  publishing service offerings, 874
  submitting requests, 880-881
Send Email Properties dialog box, 964
Send Queue % Used, 435
Send Queue % Used Top 10 report, 536-537
Sequencer (Server App-V), 753-754
Server App-V, 753
  deployment configuration files, 753
  Sequencer, 753-754
  Server App-V Agent
    definition of, 753
    installing, 754-755
    virtual environment, 753
    virtual application packages
      creating, 755-758
      definition of, 753
      importing into VMM, 758
Server Authentication certificate template, creating, 170-172
server certificates, 109
server communication, securing in Configuration Manager, 88-89
server locator functionality in Management Points, 58
Server Locator Point (SLP), 58, 85
server management suite volume licensing, 50-51
server OS deployment, 226
servers
  backups, 28-29
  database server design, 686
  DMZ servers, monitoring with certificates, 316, 385-386
    agent configuration, 392
    agent installation, 391-392
    certificate templates, creating, 386-387
    root CA server certificates, requesting, 387-390
  DPM servers
    designing, 586-587
    preparing for deployment, 587
  file servers, protecting with DPM (Data Protection Manager), 620-622
  Gateway server, 307-308
  host groups, dragging and dropping VMs onto, 752
  host servers, dragging and dropping VMs onto, 751-752
  Hyper-V servers
    backups, 31
    VMM support for, 670
  library servers, 705
management servers
  connecting to Runbook Designer, 940-941
  hardware/software requirements, 301
  installing, 934-935
  overview, 300
monitoring, 20
PXE (Preboot Execution Environment) servers, 705
Reporting Server, 304
runbook server (Orchestrator), installing, 935-937
Self-Service Portal web server design, 686
SQL Server versions, 333-334
System Center Orchestrator, 923
update servers, 705
vCenter servers, 705
VMM private cloud, 705
VMM servers, 705
  design, 686
  explained, 667
  hardware requirements, 678
  installing, 688-689, 691
  multiple-server deployment, 688
  preparing for VMM deployment, 688
  remote SQL instance requirements, 679
  single-server deployment, 688
  supported operating systems, 679
Web console, hardware/software requirements, 306
service account security (Configuration Manager), 91
service accounts (Orchestrator), 926-927
service catalog, 44
Service Level Dashboards, 293
Service Level Tracking (SLT), 293
  reports, 551-554
  SLAs (service-level agreements), 23, 548-549
  SLOs (Service Level Objectives), 549-551
Service Manager, 8, 40
  activities, 886
  announcements, publishing, 850
  architecture, 766-767
  backing up, 814
    backup schedules, 814
    database backups, 814-816
    encryption key, 816-817
  best practices, 817-818, 870
  business solutions addressed by, 41
  Change Management Pack, 764
  change requests, 885, 892-893
    creating from configuration items, 893-894
    creating from incidents or problems, 895
    creating from scratch, 893
  CMDB (configuration management database), 765
  components, 768-769
    deploying, 791-794
    explained, 765-768
service offerings, 872, 874
  creating, 879-880
  custom management packs, 875
  publishing through self-service web portals, 874
small enterprise design, 776-778
software requirements, 771-772
SQL versions, 773-774
technologies, 765
templates, 767
troubleshooting tasks, running, 851-853
workflows, 767
service monitoring, 292
service offerings (Service Manager), 872, 874
  creating, 879-880
  custom management packs, 875
  publishing through self-service web portals, 874
service requests, 44
service-level agreements (SLAs), 23, 548-549
service-level management, 44
Setup Wizard (Service Manager)
  component installation, 792-794
  data warehouse installation, 794-797
  Self-Service Portal installation, 802-804
SharePoint data backups, 30
SharePoint farms
  content databases, recovering, 649
  item-level recovery, 650-653
  preparing for protection, 644-645
  protecting with DPM, 645-647
  recovering, 647-649
  SharePoint data sources and recoverable data, 643-644
SharePoint pages, adding web parts to, 562-565
SharePoint Products and Technologies
  Configuration Wizard, 649
SharePoint web part, 290
Show Enabled Rules and Monitors for This Health Service, 439
Show Failed Rules and Monitors for This Health Service, 439
simple schedules, 106
single-server deployment (VMM), 688
single-server installations
  Operations Manager, 356-359
  Orchestrator, 928
    hardware requirements, 925
    Orchestrator Setup Wizard, 929-932
    server preparation, 929
    SQL database preparation, 929
Site Addresses, 63
site boundaries, establishing, 97-99
site codes, 63
site configuration (Configuration Manager), 148
  Asset Intelligence Synchronization Point role installation, 153-154
  Endpoint Protection Point role installation, 152-153
  FSP (Fallback Status Point) installation, 149
  OS deployment preparation, 154-155
  RSP (Reporting Service Point) installation, 149-150
  Software Update Point role installation, 150-152
Site Database, 246
Site Senders, 63
Site Servers, 62
  adding Windows roles to, 121-124
  database, 79-81
  overview, 78
Site System role changes (Configuration Manager), 58-59
sites
  discovering, 98-99
  explained, 61
  SharePoint sites, recovering, 650-653
sizing databases
  Configuration Manager, 93
  Operations Manager, 326-327
SLA report, 477
SLAs (service-level agreements), 23, 548-549
SLOs (Service Level Objectives), 549-551
slow boundaries, 97
SLP (Server Locator Point), 58, 85
SLT. See Service Level Tracking (SLT)
small enterprise design
  Configuration Manager, 110-111
  Operations Manager, 336-338
  Service Manager, 776-778
SMB-based Distribution Points, 83
SMI-S (Storage Management Initiative – Specification), 706
SMP (State Migration Point)
installing, 155
overview, 86-87
placement of, 97
SMS (Systems Management Server), 13-14
SMS Providers, 78-79
sms_def.mof editing, 59
SMTP (Simple Mail Transfer Protocol), 255
SMTP Availability report, 477
SMTP notification channels, configuring, 832-833
Software 01A - Summary of Installed Software in a Specific Collection, 273
Software 02A - Software Families, 273
Software 02B - Software Categories with a Family, 273
Software 02C - Software by Category and Family, 273
Software 02D - Computers with a Specific Software Product, 273
Software 02E - Installed Software on a Specific Computer, 273
Software 03A - Uncategorized Software, 273
Software 04A - Auto-Start Software, 273
Software 04B - Computers with a Specific Auto-Start Software, 252, 273
Software 04C - Auto-Start Software on a Specific Computer, 274
Software 05A - Browser Helper Objects, 274
Software 05B - Computers with a Specific Browser Helper Object, 274
Software 05C - Browser Helper Objects on a Specific Computer, 274
Software 06A - Search for Installed Software, 252, 274
software deployment, 12
Software Deployment section (client settings), 101, 159
software distribution. See content distribution system
software inventory, 71
Software Inventory Client Agent, 248-249
Software Inventory section (client settings), 101, 159-160
software licensing, 6, 50
core client access licenses, 50
importing license data, 275-277
server management suite volume licensing, 50-51
software metering, 73
Configuration Manager, 277-278
reports, 254
Software Metering section (client settings), 101, 160
Software Registered in Add Remove Programs on a Specific Computer report, 253
software requirements
ACS (Audit Collection Services), 311
Configuration Manager, 93
DPM (Data Protection Manager) support, 579
Gateway server, 307-308
Operations Manager, 324
agents, 301
audit collection database, 310
audit collector, 309
command shell, 307
database, 302
Operations Console, 305
Web console, 306
Reporting data warehouse, 303
Reporting Server, 304
Service Manager, 771-772
VMM Administrator Console, 680
VMM Self-Service Portal, 681
VMM server, 679
Software Update Client Agent section (client settings), 101
Software Update deployments, creating, 220-222
software update distribution (Configuration Manager), 68-69. See also update deployment
software update groups, 68
creating, 216-219
software update management, 215
creating software update groups, 216-219
viewing Update Repository, 215-216
Software Update Point (SUP)
installing, 150-152
overview, 87

How can we make this index more useful? Email us at indexes@samspublishing.com
software update reports, 253
Software Update section (client settings), 160-161
Specify Virtual Machine Identity page
   Convert Physical Server Wizard, 720
   Convert Virtual Machine Wizard, 727
SQL
   backups, 30
   choosing SQL versions, 773-774
   DPM deployment, 588
   preparing databases for System Center Orchestrator installation, 929
   versions, choosing, 104-105
   VMM support for, 679
SQL Cluster configuration (SQL Server Management Pack), 479-480
SQL Database Space report, 540-541
SQL MPDatabase State view, 483
SQL Server
   databases
      protecting with DPM, 636-638
      restoring with DPM Recovery Wizard, 638-640
      self-service restores, 640-642
   DPM support for, 579
   versions, 333-334
SQL Server Database Engine Counters report, 486
SQL Server Management Pack, 478
   configuring, 479
   reports, 486-487
   SQL Cluster configuration, 479-480
   tasks, 484-485
   tuning, 480-482
   views, 482-484
SSL, configuring
   Certificate Services website for, 174-175
   for VMM (Virtual Machine Manager) Self-Service Portal, 695
   WSUS website for, 175-176
standard activities (runbooks), 952-953
standardization, service offerings, 874
Start Audit Collection, 439
Start Online Store Maintenance, 439
Start WMI Service, 439
State Messaging section (client settings), 161
State Migration Point (SMP)
   installing, 155
   overview, 86-87
   placement of, 97
state widgets, 556-557
state-based alerting, 59
States 1 - Enforcement States for a Deployment report, 253
States 2 - Evaluation States for a Deployment report, 253
status summarizer, resetting, 128, 133
Status Summary of a Specific Task Sequence Deployment report, 254
storage
   calculating for DPM deployment, 585
   VMM private cloud, 706-707
storage area networks. See SANs (storage area networks)
Storage Management Initiative – Specification (SMI-S), 706
storage pool, adding disks to, 591-593
stored procedures, modifying, 450
submitting requests (Self-Service Web Portal), 880-881
subnets, discovering, 98-99
subscriptions
   configuring, 399-402
   notification subscriptions, 834-835
Summary page
   Convert Physical Server Wizard, 723
   Convert Virtual Machine Wizard, 728
Summary tab (Runbooks workspace), 947
SUP (Software Update Point)
   installing, 150-152
   overview, 87
suppressing reboots, 227
switches (virtual), VMware port groups for, 676
synchronizing AI (Asset Intelligence), 269-270
synthetic transaction event collection
   (Exchange 2010 Management Pack), 470-471
System activity (Orchestrator), 953
System Center Capacity Planner, 9
System Center Configuration Manager (SCCM). See Configuration Manager
System Center Data Protection Manager. See DPM (Data Protection Manager)
System Center Essentials, 9
System Center Mobile Device Manager, 9
System Center Online Services, 82
System Center Operations Manager (SCOM). See Operations Manager
System Center Orchestrator. See Orchestrator
System Center Service Manager (SCSM). See Service Manager
System Center settings (VMM Administrator Console), 715
System Center Virtual Machine Manager. See VMM (Virtual Machine Manager)
System Information page (Convert Physical Server Wizard), 720
System Integrity reports (ACS), 543
System Management container, configuring, 120-121
system monitoring, 21
system requirements
  ACS (Audit Collection Services), 311
  command shell, 307
  Configuration Manager, 92-93
  DPM (Data Protection Manager), 578-579
  Gateway server, 307-308
  Operations Manager, 323-324
    agents, 301
    audit collection database, 310
    audit collector, 309
    database, 302
    Operations Console, 305
  Reporting data warehouse, 303
  Reporting Server, 304
  virtual machine hosts, 682
  VMM Administrator Console, 679-680
  VMM Self-Service portal, 680-681
  VMM server, 678-679
  Web console, 306
System State, protecting, 622-624
systems management challenges, 6-7
Systems Management Server (SMS), 13-14
task sequences
  deployment, 59
    creating, 235-236
    reports, 254
  for MDT (Microsoft Deployment Toolkit),
    creating, 240-242
  for operating system deployment, 70
    creating, 231-234
tasks
  Active Directory Management Pack, 464
  Operations Manager Management Pack, 438-439
  SQL Server Management Pack, 484-485
  Windows Management Pack, 446-448
TCP Port Template, 501-502
technical problems addressed by VMM (Virtual Machine Manager), 665-667
templates, 889
  certificate templates, 109-110
  creating, 168-172, 386-387
  publishing, 172-173
  change request templates, 889-891
  definition of, 767
  deployment templates, 221
  Management Pack Templates, 491-492
    OLEDB Data Source Template, 497-499
    Process Monitoring Template, 499-500
    TCP Port Template, 501-502
    UNIX/Linux Log File Template, 502
    UNIX/Linux Service Template, 503
    Web Application Template, 492-494
    Windows Service Template, 494-497
  notification subscriptions, creating, 834-835
  notification templates, creating, 833-834
Terminal Services Management Pack, 425
test clients, manually compiling configuration.mof files, 265
test mailbox configuration (Exchange 2010 Management Pack), 469-470
testing runbooks, 47
  Copy File and Log Event runbook, 959-961
  Move Disabled Users runbook, 965-966
Text File Management activity (Orchestrator), 953
time estimates
  Operations Manager deployment, 353
  Service Manager projects, 791
Top X Performance reports (Operations Manager), 520-522

How can we make this index more useful? Email us at indexes@samspublishing.com
Total Usage for All Metered Software Programs report, 254
tracking
  assets, 12
  licensing, 72
  SLA (service-level agreement) tracking, 23
transact SQL (TSQL), 257
transformation, 767
Transport Platform Distribution Group Usage report, 478
Transport Platform Hourly Server Statistics report, 478
Transport Platform Server Statistics report, 478
Transport Platform Top Users report, 478
troubleshooting. See also problems
  BITS (Background Intelligent Transfer Service), 138
  extending Active Directory schema, 120
  Service Manager troubleshooting tasks, running, 851-853
Troubleshooting 1 - Scan Errors report, 253
TSQL (transact SQL), 257
tuning
  alerts, 405-409
  SQL Server Management Pack, 480-482
  Windows Management Pack, 441-443

U
UMLocal Service report, 478
Unified Messaging role, 476
UNIX agents, installing, 379-385
UNIX/Linux Log File Template, 502
UNIX/Linux Service Template, 503
unknown computers, importing, 234-235
update deployment, 11, 219
  automatic deployment rules, creating, 222-224
  deployment packages, creating, 219-220
  monitoring, 224-225
  Software Update deployments, creating, 220-222
update lists. See software update groups
update management. See software update management
Update Repository, viewing, 215-216
update schedules for collections, 187
update servers, 705
updating management packs, 404-405
Usage reports (ACS), 544
User and Device Affinity section (client settings), 161-162
User Device Affinity Associations per Collection report, 252
user notification change requests, 908-910
user roles (VMM), 672-673, 729
  Administrator, 729-731
  Delegated Administrator, 729, 732-734
  Read-Only Administrator, 730, 734-735
  Self-Service User
    creating, 735-739
    explained, 730
    modifying, 739-740
    removing, 740
user self-service (service offerings), 874
user state, capturing, 231
User State Migration Tool, creating package for, 227-228
users, targeting, 203-207
Utilities activity (Orchestrator), 953

V
V2V (virtual-to-virtual) conversions, 36, 725-729
validating
  Central Administration Site installation, 127-129
  custom inventory data, 267-268
  Enterprise Root CA, 165
  Primary Site Server installation, 131-133
  processes, 48
  secondary site installation, 136-138
vCenter servers, 705
VDS (Virtual Disk Service), 707
Veritas Storage Foundation 5.1 for Windows, 676
viewing
  custom inventory data, 268
  data warehouse job schedules, 799-800
  Operations Manager dashboards, 559-560
  Update Repository, 215-216
views
  Active Directory Management Pack, 460-463
  Cross Platform Management Packs, 488-489
  Dashboard views, 290
Exchange 2010 Management Pack, 471-477
Operations Manager Management Pack, 434-437
SQL Server Management Pack, 482-484
Windows Management Pack, 443-445
VIP (virtual IP) templates, 706
Virtual Machine Configuration page
Virtual Machine Manager. See VMM (Virtual Machine Manager)
virtual machines. See Hyper-V virtual machines;
VMs (virtual machines)
virtual switches, VMware port groups for, 676
virtual-to-virtual (V2V) conversions, 36, 725-729
VMM (Virtual Machine Manager), 8
Administrator Console, 679-680
best practices, 701-702, 759-760
business solutions addressed by, 35-36, 664-665
cluster support, 671
components, 667
deploying
multiple-server deployment, 688
single-server deployment, 688
VMM Administrator Console installation, 692-693
VMM Agent installation, 695-700
VMM Self-Service Portal installation, 694
VMM Self-Service Portal security, 695
VMM server installation, 688-691
VMM server preparation, 688
fabric management, 677, 686
heterogeneous VM management, 670
hosts
host clusters, 710
host groups, 705, 708-709
managing, 709
major features of, 36-38
new features, 39, 677-678
overview, 8, 34-35, 663-664
planning for, 682
database server and database
design, 686
environment, 682-683
infrastructure fabric, 686-687
library server and library design, 687
Operations Manager integration, 684
project scope, 683-684
Self-Service Portal web server
design, 686
VMM instances, 685
VMM server design, 686
PowerShell support, 669-670
private clouds
creating, 711-714
explained, 704
fabric resources, 704
networks, 706
servers, 705
storage, 706-707
revisions and product history, 38, 673-677
early virtualization management
techniques, 673
Virtual Machine Manager 2007, 673-674
Virtual Machine Manager 2008, 674
Virtual Machine Manager 2008 R2, 674-677
role-based access control, 672-673
Self-Service Portal
creating VMs with, 745-747
hardware requirements, 680
software requirements, 681
supported operating systems, 681
web server design, 686
Self-Service User role, 673
Server App-V, 753
deployment configuration files, 753
Sequencer, 753-754
Server App-V Agent, 753-755
virtual application packages, 753-758
virtual environment, 753
technical problems addressed by, 665-667
user roles, 729
Administrator, 729-731
Delegated Administrator, 729, 732-734
modifying, 739-740
How can we make this index more useful? Email us at indexes@samspublishing.com
Read-Only Administrator, 730, 734-735
removing, 740
Self-Service User, 730, 735-739
virtual machine hosts, system requirements, 682
VMM Administrator Console, 707-708
configuring VMM library, 710-711
creating host groups, 708-709
creating private clouds, 711-714
deploying VMs, 742-744
explained, 668
General settings, 715
managing host clusters, 710
managing hosts, 709
managing VMs, 714
monitoring and reporting, 714
Security settings, 715
System Center settings, 715
VMM Administrator role, 672, 729-731
VMM Agent
explained, 668
installing, 695-700
VMM command shell, 715-716
VMM Delegated Administrator role, 672, 729, 731-734
VMM library
configuring, 710-711
designing, 687
explained, 668-669
VMM Self-Service Portal
explained, 668
installing, 694
security, 695
VMM servers, 705
designing, 686
explained, 667
hardware requirements, 678
installing, 688-693
remote SQL instance requirements, 679
software requirements, 679
supported operating systems, 679
VMM Setup Wizard
VMM Administrator Console installation, 692-693
VMM Self-Service Portal installation, 694
VMM server installation, 689-691
VMs (virtual machines)
creating with Self-Service Portal, 745-747
customizing host ratings for, 741-742
deploying with Administrator Console, 742-744
managing, 714
migrating
by dragging and dropping onto host group, 752
by dragging and dropping onto host server, 751-752
with Migrate action, 748-750
with Migrate Storage action, 750-751
supported storage migration technologies, 748
supported VM migration technologies, 747-748
monitoring and reporting, 714
P2V (physical-to-virtual) conversions, 717-724
placement, 740-741
V2V (virtual-to-virtual) conversions, 725-729
VMware
port groups for virtual switches, 676
VMM support for, 670
Volume Configuration page (Convert Physical Server Wizard), 721

W–Z
Wake On LAN functionality, 81
Web Access Confirmation dialog box, 388-389
Web Application Template, 492-494
Web console, 422-425
hardware/software requirements, 306
overview, 305-306
Performance view time frame, 410-411
Web Page view (Operations console), 424
web parts
Operations Manager Dashboard Viewer web part
adding to SharePoint page, 562-565
configuring, 562
deploying, 561-562
SharePoint web part, 290
web services (Orchestrator), installing, 937-938
widgets
  adding to dashboards, 557-559
  explained, 556
Windows agents, installing, 373-376
Windows Authentication, configuring for VMM
  Self-Service Portal, 695
Windows Core OS monitoring, management
  packs, 440
Windows Installer, 189
  configuring MSI applications, 191-192
Windows Management Instrumentation (WMI), 245
Windows Management Pack, 440
  configuring, 440-441
  reports, 448-451
  tasks, 446-448
  tuning, 441-443
  views, 443-445
Windows PowerShell
  attaching protection agents with, 601
  cmdlets, 290
  VMM support for, 669-670, 677
Windows roles, adding on Site Servers, 121-124
Windows Server 2008 Core Operating System
  object, 442
Windows Server 2008 Logical Disk object, 442
Windows Server 2008 Network Adapter
  object, 443
Windows Server performance reports, 523-524
Windows Server Update Services (WSUS),
  11, 150
Windows Service Template, 494-497
WinPE environment, 69
wizards. See names of specific wizards
WMI (Windows Management Instrumentation), 245
WOL (Wake On LAN) functionality, 81
workflow engine, 765
workflows, 767, 889-892
workspaces
  Orchestration console, 947-948
  Runbook Designer, 944-945
WSSCmdletsWrapper, 645
WSUS (Windows Server Update Services),
  11, 150
WSUS website, configuring for SSL, 175-176
XML management pack, modifying, 506

How can we make this index more useful? Email us at indexes@samspublishing.com