



Implementing an Advanced Server Infrastructure

Exam Ref 70-414

Steve Suehring

Exam Ref 70-414 Implementing an Advanced Server Infrastructure

Steve Suehring

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Copyright © 2014 by Steve Suehring

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

Library of Congress Control Number: 2014940676
ISBN: 978-0-7356-7407-3

Printed and bound in the United States of America.

First Printing

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at mspinput@microsoft.com. Please tell us what you think of this book at <http://www.microsoft.com/learning/booksurvey>.

Microsoft and the trademarks listed at <http://www.microsoft.com/en-us/legal/intellectualproperty/Trademarks/EN-US.aspx> are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

The example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation, nor its resellers, or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Acquisitions Editor: Anne Hamilton
Developmental Editor: Karen Szall
Editorial Production: Box Twelve Communications
Technical Reviewer: Brian Svidergol
Cover: Twist Creative • Seattle

Contents at a glance

	<i>Introduction</i>	<i>xi</i>
	<i>Preparing for the exam</i>	<i>xv</i>
CHAPTER 1	Manage and maintain a server infrastructure	1
CHAPTER 2	Plan and implement a highly available enterprise infrastructure	53
CHAPTER 3	Plan and implement a server virtualization infrastructure	117
CHAPTER 4	Design and implement identity and access solutions	189
	<i>Index</i>	<i>263</i>

This page intentionally left blank

Contents

Introduction	xi
<i>Microsoft certifications</i>	<i>xii</i>
<i>Acknowledgments</i>	<i>xii</i>
<i>Errata & book support</i>	<i>xii</i>
<i>We want to hear from you</i>	<i>xii</i>
<i>Stay in touch</i>	<i>xiii</i>
Preparing for the exam	xv
Chapter 1 Manage and maintain a server infrastructure	1
Objective 1.1: Design an administrative model	1
Understanding administrative model design considerations	2
Understanding delegation in System Center 2012 R2	11
Understanding self-service portal design using Service Manager	18
Delegating rights for the private cloud	19
Objective summary	21
Objective review	21
Objective 1.2: Design a monitoring strategy	22
Enabling Audit Collection Services (ACS)	22
Understanding Global Service Monitor	25
Implementing and optimizing Operations Manager management packs	27
Planning for Active Directory monitoring	30
Objective summary	31
Objective review	31

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

www.microsoft.com/learning/booksurvey/

Objective 1.3: Plan and implement automated remediation	32
Creating an update baseline in VMM	33
Implementing a Desired Configuration Management (DCM) baseline and automatic remediation	36
Implementing VMM integration with Operations Manager	39
Configuring VMM to move a virtual machine dynamically based on policy	43
Designing and implementing a Windows PowerShell Desired State Configuration solution	45
Objective summary	47
Objective review	47
Answers	49

Chapter 2 Plan and implement a highly available enterprise infrastructure 53

Objective 2.1: Plan and implement failover clustering	53
Planning for and implementing failover clustering	54
Understanding design considerations	56
Objective summary	64
Objective review	64
Objective 2.2: Plan and implement highly available network services . . .	65
Planning for and configuring Network Load Balancing	65
Understanding design considerations	70
Objective summary	74
Objective review	75
Objective 2.3: Plan and implement highly available storage solutions . . .	76
Planning for and configuring storage spaces and storage pools	76
Designing highly available, multi-replica DFS Namespaces	82
Planning for and configuring multi-path I/O (MPIO)	88
Configuring highly available iSCSI Target and iSNS Server	90
Planning for and implementing storage using RDMA and SMB multichannel	92

Objective summary	94
Objective review	94
Objective 2.4: Plan and implement highly available server roles	95
Planning for highly available services	95
Planning and implementing highly available applications, services, and scripts	98
Objective summary	99
Objective review	100
Objective 2.5: Plan and implement a business continuity and disaster recovery solution	100
Planning a backup and recovery strategy	101
Understanding planning considerations	102
Planning for and implementing backup and recovery using System Center Data Protection Manager (DPM)	104
Objective summary	111
Objective review	112
Answers	113

Chapter 3 Plan and implement a server virtualization infrastructure 117

Objective 3.1: Plan and implement virtualization hosts	117
Planning for and implementing virtual environment delegation	118
Planning and implementing multi-host libraries	125
Planning for and implementing host resource optimization	127
Integrating third-party virtualization platforms	129
Deploying Hyper-V hosts to bare metal	130
Objective summary	131
Objective review	131
Objective 3.2: Plan and implement virtual machines	132
Planning and implementing highly available VMs	132
Planning for and implementing guest resource optimization	134
Configuring placement rules	136
Creating Virtual Machine Manager templates	140

Objective summary	144
Objective review	145
Objective 3.3: Plan and implement virtualization networking	146
Planning for and configuring Virtual Machine Manager logical networks	146
Planning for and configuring IP address and MAC address settings across multiple Hyper-V hosts	150
Planning for and configuring network optimization	156
Planning for and implementing Windows Server Gateway	157
Objective summary	157
Objective review	158
Objective 3.4: Plan and implement virtualization storage.	159
Planning for and configuring Hyper-V host clustered storage	159
Planning for and configuring Hyper-V guest storage	162
Planning for storage optimization	163
Objective summary	164
Objective review	164
Objective 3.5: Plan and implement virtual machine movement.	165
Planning for and configuring live and storage migration between Hyper-V hosts and clouds	165
Planning for and managing P2V and V2V	168
Objective summary	171
Objective review	171
Objective 3.6: Manage and maintain a server virtualization infrastructure	172
Managing dynamic optimization and resource optimization	172
Integrating Operations Manager with VM and Service Manager	175
Update virtual machine images in libraries	179
Planning for and implementing backup and recovery of virtualization infrastructure using DPM	180
Objective summary	181
Objective review	182
Answers.	183

Chapter 4 Design and implement identity and access solutions 189

Objective 4.1: Design a Certificate Services infrastructure	189
Designing a multi-tier certification authority hierarchy	190
Planning for multi-forest CA deployment and trust between organizations	192
Planning for Certificate Enrollment Web Services	192
Planning for Network Device Enrollment Services (NDES)	193
Planning for certificate validation and revocation	193
Planning for disaster recovery	194
Objective summary	195
Objective review	195
Objective 4.2: Implement and manage a Certificate Services infrastructure	196
Configuring and managing offline root CA	196
Configuring and managing Certificate Enrollment Web Services and Certificate Enrollment Policy Web Services	201
Configuring and managing Network Device Enrollment Services (NDES)	204
Configuring Online Certificate Status Protocol (OCSP) responders	205
Migrating the CA	209
Implementing administrator role separation	209
Implementing and managing trust between organizations	211
Monitoring CA health	214
Objective summary	216
Objective review	216
Objective 4.3: Implement and manage certificates	217
Managing certificate templates	217
Implementing and managing certificate deployment, validation, renewal, and revocation	221
Managing certificate renewal	223
Configuring and managing key archive and recovery	225
Objective summary	227
Objective review	228

Objective 4.4: Design and implement a federated identity solution . . .	228
Planning for and implementing claims-based authentication	229
Planning for and configuring claims provider and relying-party trust claim rules	232
Planning for and configuring attribute stores	235
Planning for and managing Active Directory Federation Services (AD FS) certificates	237
Planning for and implementing Identity Integration with cloud services	238
Integrating Web Application Proxy with AD FS	239
Objective summary	241
Objective review	241
Objective 4.5: Design and implement Active Directory Rights Management Services (AD RMS)	242
Planning for highly available AD RMS deployment	242
Planning for and managing AD RMS client deployment	245
Managing trusted user domains	247
Managing trusted publishing domains	249
Managing federated identity support	250
Upgrading, migrating, and decommissioning AD RMS	254
Objective summary	256
Objective review	256
Answers	258
 <i>Index</i>	 263

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

www.microsoft.com/learning/booksurvey/

Introduction

This book covers the 70-414 certification exam, “Implementing an Advanced Server Infrastructure.” More specifically, the book examines the second revision, or “R2,” edition of the exam objectives. The book is written for IT professionals who already have experience with Windows networks.

The 70-414 exam covers advanced topics that IT professionals encounter in the enterprise environment. Topics such as monitoring, virtualization, and high availability are emphasized in the exam objectives. You should have a thorough understanding of a basic server infrastructure as a prerequisite for this book and the 70-414 exam.

There are four main objective areas on the 70-414 exam and each area is covered to a differing level:

- Manage and maintain a server infrastructure: 25 to 30 percent
- Plan and implement a highly available enterprise infrastructure: 25 to 30 percent
- Plan and implement a server virtualization infrastructure: 20 to 30 percent
- Design and implement identity and access solutions: 20 to 25 percent

As you can see from the broad objective areas, there is coverage of both planning and implementation as well as management and design. This level of coverage means that you'll likely need to be able to choose an appropriate solution given a specific scenario or set of technologies for that scenario. Once chosen, you'll then need to be able to determine the most successful path for implementation.

This book covers every exam objective, but it does not cover every exam question. Only the Microsoft exam team has access to the exam questions, and Microsoft regularly adds new questions to the exam, making it impossible to cover specific questions. You should consider this book a supplement to your relevant real-world experience and other study materials. If you encounter a topic in this book that you do not feel completely comfortable with, use the links you'll find in the text to find more information and take the time to research and study the topic. Great information is available on MSDN, TechNet, and in blogs and forums.

Microsoft certifications

Microsoft certifications distinguish you by proving your command of a broad set of skills and experience with current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies both on-premises and in the cloud. Certification brings a variety of benefits to the individual and to employers and organizations.

MORE INFO ALL MICROSOFT CERTIFICATIONS

For information about Microsoft certifications, including a full list of available certifications, go to <http://www.microsoft.com/learning/en/us/certification/cert-default.aspx>.

Acknowledgments

Thanks to Karen Szall and the Microsoft Press team, as well as Jeff Riley. It's been a pleasure working with you all, as always.

Free ebooks from Microsoft Press

From technical overviews to in-depth information on special topics, the free ebooks from Microsoft Press cover a wide range of topics. These ebooks are available in PDF, EPUB, and Mobi for Kindle formats, ready for you to download at:

<http://aka.ms/mspressfree>

Check back often to see what is new!

Errata, updates, & book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

<http://aka.ms/ER414R2>

If you discover an error that is not already listed, please submit it to us at the same page.

If you need additional support, email Microsoft Press Book Support at msspinput@microsoft.com.

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to *<http://support.microsoft.com>*.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

<http://aka.ms/tellpress>

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in touch

Let's keep the conversation going! We're on Twitter: <http://twitter.com/MicrosoftPress>.

This page intentionally left blank

Preparing for the exam

Microsoft certification exams are a great way to build your resume and let the world know about your level of expertise. Certification exams validate your on-the-job experience and product knowledge. While there is no substitution for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam. We recommend that you round out your exam preparation plan by using a combination of available study materials and courses. For example, you might use this Exam Ref and another study guide for your “at home” preparation and take a Microsoft Official Curriculum course for the classroom experience. Choose the combination that you think works best for you.

Note that this Exam Ref is based on publicly available information about the exam and the author’s experience. To safeguard the integrity of the exam, authors do not have access to the live exam.

This page intentionally left blank

Manage and maintain a server infrastructure

The 70-414 exam looks to stretch your understanding of planning, implementation, and management of an advanced Microsoft-based infrastructure. The tools and products included in the exam are used in enterprise-level networks and emphasize automation, high availability, and self-service. The first chapter of this book discusses objectives surrounding server infrastructure management. Within this chapter and indeed the entire book, you'll find hands-on examples that directly tie to the exam objectives, and you'll find numerous links to more information on TechNet.

Objectives in this chapter:

- Objective 1.1: Design an administrative model
- Objective 1.2: Design a monitoring strategy
- Objective 1.3: Plan and implement automated remediation

IMPORTANT

Have you read page xv?

It contains valuable information regarding the skills you need to pass the exam.

Objective 1.1: Design an administrative model

Designing an administrative model for an enterprise network involves a large amount of planning, especially in complex or highly structured enterprises. A good administrative model will enable delegation of authority while also enforcing the principle of least privilege. Many organizations have unique needs, but the overall administrative model can follow a common pattern. For example, an organization that's geographically dispersed may allow personnel at remote locations to change passwords for users at that remote site.

This objective covers how to:

- Understand design considerations, including user rights and built-in groups
- Understand designing a delegation of administration structure for System Center 2012 R2
- Understand self-service portal design using System Center 2012 Service Manager
- Delegate rights for managing private clouds by using System Center 2012 App Controller and Virtual Machine Manager

Understanding administrative model design considerations

Typical enterprise administrative and privilege models use groups to assign and delegate permissions. Groups save time and administration overhead by combining similar users and computers into one entity that can then be assigned permissions.

MORE INFO DESIGN STRATEGIES FOR ACTIVE DIRECTORY DOMAIN SERVICES (AD DS)

This section examines user rights and built-in groups. If you're unfamiliar with design strategies for Active Directory Domain Services (AD DS), you can find more information in the AD DS Design Guide at <http://technet.microsoft.com/library/cc754678.aspx>.

Groups can have users and computers and are created as a security group or a distribution group. The security group type is covered in this chapter; distribution groups are typically used to create email distribution lists and aren't covered in this book. Groups are also scoped, which means that they can apply locally to a computer, to a domain, or to an entire forest. Table 1-1 describes the three types of group scopes available in AD DS.

TABLE 1-1 Active Directory Domain Services group scope

Group Scope	Description
Domain Local	Members in a Domain Local scoped group can have permissions within the same domain where the Domain Local group is located and can contain any combination of groups with domain local, global, or universal scope.
Global	Members of groups with a Global scope can have permissions in any domain within a forest, but members can come from only the domain within which the group is defined.
Universal	Members of groups with Universal scope can have permissions in any domain or forest and can originate from any domain or forest.

User rights

Before looking at user rights, it's important to agree on the definition of a user right. You can find a definition all the way back to Windows NT Server 4.0 in the "NT Server 4.0 Concepts and Planning Manual" on TechNet, where a *right* is defined as something that "authorized a user to perform certain actions on a computer system." See <http://technet.microsoft.com/en-us/library/cc751446.aspx> for more discussion on the definition.

What's important to realize is the distinction between a right and a permission. A *right* defines what a user can do on a computer system, whereas *permissions* apply to objects. Rights can override permissions in certain instances. For example, if a user is a member of a group that has the right to back up a computer or has the Back Up Files and Directories right, that user inherently has read access to the files on the computer, even if permissions would normally deny such access. More specifically, the Back Up Files and Directories right has the following permissions:

- Traverse Folder/Execute File
- List Folder/Read Data
- Read Attributes
- Read Extended Attributes
- Read Permissions

The Back Up Files and Directories right is just one example of this concept. Table 1-2 shows several other security-related user rights available with Windows Server 2012. An abbreviated constant name applies to each of the rights described in Table 1-2. The constant names are used for logging and can also be used for Windows PowerShell, as discussed later in this section.

TABLE 1-2 Additional security-related user rights

User Right	Description	Constant Name
Access Credential Manager as a trusted caller	Applies to Credential Manager during backup-related processes. This privilege is assigned to the Winlogon service only and should not be assigned to the account.	SeTrustedCredManAccessPrivilege
Access this computer from the network	Determines whether a user can utilize protocols related to accessing a given computer, such as Service Message Block (SMB), NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+).	SeNetworkLogonRight
Act as part of the operating system	Applies to processes to determine whether they can use a user's identity to gain access to the privileges granted to that user.	SeTcbPrivilege

User Right	Description	Constant Name
Add workstations to domain	Enables a user to add a computer to a domain.	SeMachineAccountPrivilege
Adjust memory quotas for a process	Enables a user to change the memory used by a process.	SeIncreaseQuotaPrivilege
Allow logon locally	Enables a user to start an interactive session.	SeInteractiveLogonRight
Allow logon through Remote Desktop Services	Enables a user to log on using Remote Desktop Services.	SeRemoteInteractiveLogonRight
Back up files and directories	Enables an account to bypass permissions for backup purposes.	SeBackupPrivilege
Bypass traverse checking	Enables an account to traverse an NTFS file system without needing to check the Traverse Folder permission.	SeChangeNotifyPrivilege
Change the system time	Enables a user to change the time on the local computer.	SeSystemtimePrivilege
Change the time zone	Enables a user to change the time zone on the local computer.	SeTimeZonePrivilege
Create a pagefile	Enables a user to change settings around the pagefile, including its size.	SeCreatePagefilePrivilege
Create a token object	Enables a process to create a token using the privileged account.	SeCreateTokenPrivilege
Create global objects	Enables creation of global objects.	SeCreateGlobalPrivilege
Create permanent shared objects	Enables creation of directory objects.	SeCreatePermanentPrivilege
Create symbolic links	Enables an account to create a file system symbolic link.	SeCreateSymbolicLinkPrivilege
Debug programs	Enables a user to attach to a process for debugging.	SeDebugPrivilege
Deny access to this computer from the network	Prevents users from accessing the computer.	SeDenyNetworkLogonRight
Deny logon as a batch job	Prevents an account from logging on using batch-related methods.	SeDenyBatchLogonRight
Deny logon as a service	Prevents an account from logging on as a service.	SeDenyServiceLogonRight
Deny logon locally	Prevents an account from logging on locally at a computer console.	SeDenyInteractiveLogonRight
Deny logon through Remote Desktop Services	Prevents users from logging on to a computer using Remote Desktop Services.	SeDenyRemoteInteractiveLogonRight

User Right	Description	Constant Name
Enable computer and user accounts to be trusted for delegation	Enables a user to set the Trusted for Delegation setting.	SeEnableDelegationPrivilege
Force shutdown from a remote system	Allows a user to shut down a computer when connected remotely.	SeRemoteShutdownPrivilege
Generate security audits	Enables an account to generate audit records in the security log.	SeAuditPrivilege
Impersonate a client after authentication	Enables a program to impersonate a user or account and act on behalf of that user or account.	SeImpersonatePrivilege
Increase a process working set	Enables a user to increase the size of a working set of a process.	SeIncreaseWorkingSetPrivilege
Increase scheduling priority	Enables a user to increase the base priority of a process.	SeIncreaseBasePriorityPrivilege
Load and unload device drivers	Enables a user to dynamically load or unload device drivers.	SeLoadDriverPackage
Lock pages in memory	Enables an account to keep data from a process in physical memory.	SeLockMemoryPrivilege
Log on as a batch job	Enables an account to log on using batch-related methods, including Task Scheduler.	SeBatchLogonRight
Log on as a service	Enables a service account to register a process.	SeServiceLogonRight
Manage auditing and security log	Enables a user to work with auditing and security log.	SeSecurityPrivilege
Modify an object label	Enables an account to modify integrity labels used by Windows Integrity Controls (WIC).	SeRelabelPrivilege
Modify firmware environment values	Enables a user to modify non-volatile RAM (NVRAM) settings.	SeSystemEnvironmentPrivilege
Perform volume maintenance tasks	Enables a user to do volume- and disk management–related tasks.	SeManageVolumePrivilege
Profile single process	Enables a user to view performance aspects of a process.	SeProfileSingleProcessPrivilege
Profile system performance	Enables a user to use the Windows Performance Monitor tools.	SeSystemProfilePrivilege
Remove computer from docking station	Enables a user to undock a computer without logging on.	SeUndockPrivilege
Replace a process level token	Enables a process to replace an access token of a child process.	SeAssignPrimaryTokenPrivilege
Restore files and directories	Enables a user to bypass the normal permission checks when restoring.	SeRestorePrivilege

User Right	Description	Constant Name
Shut down the system	Enables a local user to shut down the system.	SeShutdownPrivilege
Synchronize directory service data	Enables a user to synchronize service data, such as LDAP directory synchronization.	SeSyncAgentPrivilege
Take ownership of files or other objects	Enables an account to take ownership of objects in the computer.	SeTakeOwnershipPrivilege

The constant name described in Table 1-2 can be used with Windows PowerShell cmdlets related to privileges:

- Get-Privilege
- Grant-Privilege
- Revoke-Privilege
- Test-Privilege

As described in Table 1-2, user rights generally shouldn't be applied to accounts directly, but rather should be granted through the use of groups.

MORE INFO USER RIGHTS ASSIGNMENT

See <http://technet.microsoft.com/library/dn221963> for more information on user rights assignment.

Built-in groups

Built-in groups, also called *default groups*, are added with the operating system. Many of the default groups have user rights assigned already. Certain rights also apply depending on the type of computer on which the right is being exercised. For example, the Allow Logon Locally right is granted to the following groups for logging on to workstations and servers:

- Administrators
- Backup Operators
- Users

By contrast, the following groups have the Allow Logon Locally right for domain controllers:

- Account Operators
- Administrators
- Backup Operators
- Print Operators
- Server Operators

Table 1-3 shows the local groups for a computer and the user rights granted to them by default.

TABLE 1-3 User rights for local groups

Group	User Rights
Administrators	Access this computer from the network Adjust memory quotas for a process Allow logon locally Allow logon through Remote Desktop Services Back up files and directories Bypass traverse checking Change the system time Change the time zone Create a page file Create global objects Create symbolic links Debug programs Force shutdown from a remote system Impersonate a client after authentication Increase scheduling priority Load and unload device drivers Log on as a batch job Manage auditing and security log Modify firmware environment variables Perform volume maintenance tasks Profile system performance Remove computer from docking station Restore files and directories Shut down the system Take ownership of files or other objects
Backup Operators	Access this computer from the network Allow logon locally Back up files and directories Bypass traverse checking Log on as a batch job Restore file and directories Shut down the system
Cryptographic Operators	No user rights granted by default
Distributed COM Users	No user rights granted by default
Guests	No user rights granted by default
IIS_IUSRS	No user rights granted by default
Network Configuration Operators	No user rights granted by default
Performance Log Users	No user rights granted by default
Performance Monitor Users	No user rights granted by default
Power Users	No user rights granted by default
Remote Desktop Users	Allow logon through Remote Desktop Services
Replicators	No user rights granted by default

Group	User Rights
Users	Access this computer from the network Allow logon locally Bypass traverse checking Change the time zone Increase a process working set Remove the computer from a docking station Shut down the system
Offer Remote Assistance Helpers	No user rights granted by default

MORE INFO DEFAULT LOCAL GROUPS

See <http://technet.microsoft.com/library/cc771990.aspx> for more information on default local groups.

AD DS also contains default groups. These groups are placed into either the Builtin or Users container.

Table 1-4 describes the groups in the Builtin container.

TABLE 1-4 Groups in the Builtin container

Group	User Rights
Account Operators	Allow logon locally Shut down the system
Administrator	Access this computer from the network Adjust memory quotas for a process Back up files and directories Bypass traverse checking Change the system time Create a pagefile Debug programs Enable computer and user accounts to be trusted for delegation Force a shutdown from a remote system Increase scheduling priority Load and unload device drivers Allow logon locally Manage auditing and security log Modify firmware environment values Profile single process Profile system performance Remove computer from docking station Restore files and directories Shut down the system Take ownership of files or other objects
Backup Operators	Back up files and directories Allow logon locally Restore files and directories Shut down the system
Guests	No user rights granted by default

Group	User Rights
Incoming Forest Trust Builders	No user rights granted by default; applicable to forest root domain only
Network Configuration Operators	No user rights granted by default
Performance Monitor Users	No user rights granted by default
Performance Log Users	No user rights granted by default
Pre-Windows 2000 Compatible Access	Access this computer from the network Bypass traverse checking
Print Operators	Allow logon locally Shut down the system
Remote Desktop Users	No user rights granted by default
Replicator	No user rights granted by default
Server Operators	Back up files and directories Change the system time Force shutdown from a remote system Allow logon locally Restore files and directories Shut down the system
Users	No user rights granted by default

Table 1-5 describes the groups in the Users container.

TABLE 1-5 Groups in the Users container

Group	User Rights
Cert Publishers	No user rights granted by default
DnsAdmins	No user rights granted by default; installed as part of DNS
DnsUpdateProxy	No user rights granted by default; installed as part of DNS
Domain Admins	Access this computer from the network Adjust memory quotas for a process Back up files and directories Bypass traverse checking Change the system time Create a pagefile Debug programs Enable computer and user accounts to be trusted for delegation Force a shutdown from a remote system Increase scheduling priority Load and unload device drivers Allow logon locally Manage auditing and security log Modify firmware environment values Profile single process Profile system performance Remove computer from docking station Restore files and directories Shut down the system Take ownership of files or other objects

Group	User Rights
Domain Computers	No user rights granted by default
Domain Controllers	No user rights granted by default
Domain Guests	No user rights granted by default
Domain Users	No user rights granted by default
Enterprise Admins	Note: Permissions are applicable to forest root domain only Access this computer from the network Adjust memory quotas for a process Back up files and directories Bypass traverse checking Change the system time Create a pagefile Debug programs Enable computer and user accounts to be trusted for delegation Force a shutdown from a remote system Increase scheduling priority Load and unload device drivers Allow logon locally Manage auditing and security log Modify firmware environment values Profile single process Profile system performance Remove computer from docking station Restore files and directories Shut down the system Take ownership of files or other objects
Group Policy Creator Owners	No user rights granted by default
IIS_WPG	No user rights granted by default; installed with IIS
RAS and IAS Servers	No user rights granted by default
Schema Admins	No user rights granted by default; applicable to forest root domain only

Built-in groups are different from special identities. A special identity is a group for which membership cannot be modified, such as the Everyone group. Special identities include those in Table 1-6.

TABLE 1-6 Special identities

Identity	Description
Anonymous Logon	Used for anonymous access to services and resources
Everyone	All network users, with the exception of the Anonymous Logon group
Interactive	Users who are logged on locally to the computer
Network	Users who are accessing a computer's resources over the network

MORE INFO SPECIAL IDENTITIES

See <http://technet.microsoft.com/en-us/library/cc733001> for more information on special identities.

Understanding delegation in System Center 2012 R2

Microsoft System Center 2012 R2 consists of several products, including Configuration Manager, Operations Manager, Data Protection Manager, Service Manager, AppController, and Virtual Machine Manager (VMM). The products used in the organization determine the delegation structure. For example, certain roles are only applicable for Virtual Machine Manager and others are applicable for Configuration Manager. If the organization doesn't use VMM, then those roles wouldn't be used. However, the concepts of delegated authority and role-based administration are applicable no matter what products are being used. This section examines delegation for Configuration Manager and Operations Manager. Other products such as Virtual Machine Manager and Data Protection Manager are covered in other objectives in this chapter.

Role-based administration

System Center 2012 R2 uses role-based administration to facilitate the structure needed in many organizations. Using role-based administration you can limit the authority and scope of permissions to the least amount necessary in order to complete a task. For example, an organization may grant the ability to change passwords for normal users to help desk staff. This scenario can be accomplished by granting the limited privileges to the help desk personnel. An important concept surrounding role-based administration in System Center is administrative scope. Administrative scope defines the permissions that a given user has on objects within the scope's control. Administrative scopes consist of:

- Security roles
- Collections
- Security scopes

MORE INFO ROLE-BASED ADMINISTRATION

See http://technet.microsoft.com/en-us/library/65fffa65-5c09-4f6c-82bf-e01d567cda20#BKMK_PlanningForRBA for more information on role-based administration planning.

SECURITY ROLES

Security roles, which you might think of like a group in Active Directory, are used to grant sets of permissions to users based on their role. For example, the Asset Analyst role is granted certain permissions to view Asset Intelligence and inventory information. Users can then be given the Asset Analyst role to do their job.

Each security role is granted specific permissions, such as Approve, Create, Delete, Modify, and so on. The permissions apply to specific object types within System Center. There are several built-in security roles that come with Configuration Manager and with other System Center products. The permissions granted to these roles can't be changed. However, the roles can be copied, and a new role can be built and modified as needed.

The general steps for planning security roles are:

1. Identify tasks. Examine the responsibilities for administrators. For example, you might have administrators that are responsible for client security while others are responsible for software updates.
2. Map tasks to roles. Determine how the responsibilities connect to built-in security roles.
3. Assign roles. Assign roles to users. If a user has responsibilities across multiple roles, assign that user to multiple roles.
4. Create new roles (optional). Create new roles if the responsibilities don't map to one or more of the built-in roles.

COLLECTIONS

Computers and users are grouped into collections in Configuration Manager. Collections are important in the hierarchical delegation of administration for Configuration Manager. Collections can be created to meet the needs of the organization. For example, you might create a collection for each physical location in an organization, or you might create a functional collection that includes all servers or all client computers. Like security roles, there are several built-in collections that can't be modified. Collections become very useful when you want to distribute software, provide reporting, or ensure configuration changes are consistent across the devices within the collection.

MORE INFO COLLECTIONS

See <http://technet.microsoft.com/en-us/library/gg682177> for more information on collections.

SECURITY SCOPES

Security scopes can be used to grant access to securable objects by type. Security scopes provide granular access control. However, security scopes can't be nested or used in a hierarchical manner. Security scopes are useful for segregating objects of the same type so that different levels of access can be granted to them. For instance, if a set of administrators should be granted full access only to non-production servers, the servers can be scoped to separate production from development servers.

There are two built-in security scopes:

- **All** Includes all scopes. Objects cannot be added to this scope.
- **Default** Installed with Configuration Manager, the default scope also includes all objects.



EXAM TIP

Security scopes are configured within Configuration Manager in the Set Security Scopes dialog box found in the Classify group.

Certain objects can't be secured by security scopes. Instead, access to these objects is granted using security roles. Objects that can't be included in security scopes are:

- Active Directory forests
- Administrative users
- Alerts
- Boundaries
- Computer associations
- Default client settings
- Deployment templates
- Device drivers
- Exchange server connectors
- Migration site-to-site mappings
- Mobile device enrollment profiles
- Security roles
- Security scopes
- Site addresses
- Site system roles
- Software titles
- Software updates
- Status messages
- User device affinities

Delegation design

Hierarchical structure is important for designing a delegated administration for System Center. When it is properly structured, you can delegate responsibilities merely by using scopes and security roles. However, as the organization's needs change, so too will the needs for delegated administration. For example, if a merger takes place, the newly merged company may need to manage its own site.

Designing delegation involves determining the following:

- **Who** Who is responsible for managing a given client computer or server? Determine the various tasks involved in administration, whether that's software updates, security, or anything else that System Center can do. These tasks will map to security roles.
- **Which and Where** Which computers, servers, or other objects will those people manage, based on their roles? Where are those objects located, both physically and logically? For instance, there may be different responsibilities based on physical location or logical location (production versus test). Collections are used to group the objects together in Configuration Manager, and security scopes can be used to provide more granular control over the objects.
- **What** What permissions do administrators need on a given object? Permissions can be changed within the security roles, and their scope can be limited through security scopes.

Configuration Manager

System Center 2012 R2 Configuration Manager is an important piece of enterprise IT management. Configuration Manager provides a unified solution for management of operating systems, devices, software updates, asset inventory, and more. Using Configuration Manager, an enterprise can deliver software to devices within the organization and ensure consistency of updates and configurations. Configuration Manager also integrates with other System Center products and with other services like Windows Intune.

Configuration Manager can be configured as a standalone set of services or in a hierarchy, known as primary site and central administration site, respectively. The primary site-only scenario is useful for small implementations or small networks, whereas the central administration site scenario is useful for larger enterprises, especially those that need hierarchical or delegated management.

Site system roles

Within Configuration Manager, site system roles are used to define what tasks the various servers perform within a site. Site system roles shouldn't be confused with role-based administration, which is also covered in this section. Table 1-7 describes some of the typical site system roles.

TABLE 1-7 Core site system roles

Role	Description
Component server	A basic service that is responsible for running Configuration Manager services. This role is automatically installed for all roles except the distribution point role.
Site database server	The server that runs the SQL Server database and is used to store information and data related to the Configuration Manager deployment.
Site server	The server from which the core functionality of Configuration Manager is provided.
Site system	The site system role is a basic role installed on any computer hosting a site system.
SMS Provider	Provides the interface between the Configuration Manager console and the site database. Note that the SMS Provider role can be used only on computers that are in the same domain as the site server.

Multiple site system roles typically run on a single server, especially in new or small implementations of Configuration Manager. Additional servers can be deployed as distribution points to ensure availability of software packages and related files or to provide those files at strategic locations. For example, you might place a distribution point close to a large number of client computers.

Aside from the core site system roles, other site system roles may be used. Table 1-8 describes some other site system roles.

TABLE 1-8 Additional site system roles

Role	Description
Application Catalog web service point	Responsible for providing information from the Software Library to the Application Catalog website.
Application Catalog website point	A website that displays available software from the Application Catalog.
Asset Intelligence synchronization point	Exchanges Asset Intelligence information with Microsoft.
Certificate registration point	New for System Center 2012 R2, this role provides for communication for devices using Simple Certificate Enrollment Protocol (SCEP) with Network Device Enrollment Service. This role cannot exist on the same server as the computer running Network Device Enrollment Service.
Distribution point	A role that holds software packages, updates, system images, and other files for clients to download.
Endpoint Protection point	Accepts Endpoint Protection license terms and configures default membership for Microsoft Active Protection Service.
Enrollment point	Enrolls mobile devices and Mac computers using public key infrastructure and also provisions Intel Active Management Technology computers.
Enrollment point proxy	Manages enrollment requests for mobile devices and Mac computers.

Role	Description
Fallback status point	Monitors client installation and identifies clients that can't communicate with their management point.
Management point	A role that interacts with client computers to receive configuration data and send policy and service location information.
Out of band service point	Configures Intel AMT computers for out of band management.
Reporting services point	A role that creates and manages Configuration Manager reports. This role works with SQL Server Reporting Services.
Software update point	Together with Windows Software Update Services (WSUS), this role provides software updates to clients.
State migration point	Holds client user state data during migration to a new operating system.
System Health Validator point	Validates Network Access Protection (NAP) policies. The role must be installed on a NAP health policy server.
Windows Intune connector	Manages mobile devices with Windows Intune through the Configuration Manager console. This role is available with Service Pack 1 (SP1).

MORE INFO ROLE-BASED ADMINISTRATION IN CONFIGURATION MANAGER

See <http://blogs.technet.com/b/hoy/archive/2012/03/07/role-based-administration-in-system-center-2012-configuration-manager.aspx> for more information on Role-Based Administration in Configuration Manager.

Operations Manager

System Center 2012 R2 Operations Manager provides monitoring capabilities to computers across an enterprise. The roles necessary within Operations Manager include those to create monitoring configurations, view and edit reports, and provide overall administration, among others.

Operations Manager uses many of the same concepts as other System Center products for rights delegation. Operations Manager uses user roles and role profiles which are then combined with a scope to produce the user role. For example, Operations Manager has several built-in user roles, called *profiles* in Operations Manager:

- Administrator
- Advanced Operator
- Application Monitoring Operator
- Author
- Operator
- Read-only Operator
- Report Operator
- Report Security Administrator

Each of these built-in user roles can be changed through its properties settings. The scopes can be changed, as can the tasks and dashboards and views available to the user role. This is illustrated in Figure 1-1.

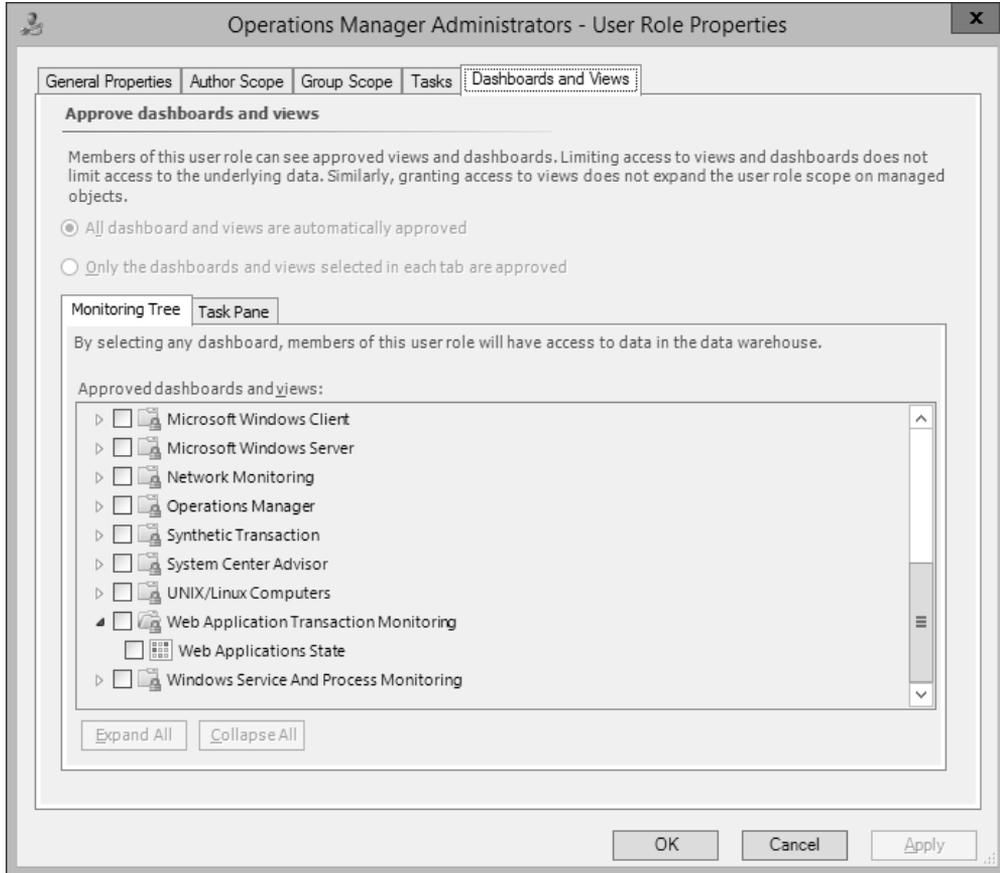


FIGURE 1-1 Changing the dashboards and views available to one of the built-in user roles in Operations Manager

Each of the built-in user roles can contain one or more local or Active Directory–based groups or users. For example, the Operations Manager Administrators user role (shown in Figure 1-1) contains the BUILTIN\Administrators group.

You can also create user roles within Operations Manager by using the Create User Role Wizard. When creating a new user role you first choose the type of user role on which the new user role will be based from among these choices:

- Operator
- Read-Only Operator
- Author
- Advanced Operator

Each of these profiles provides certain privileges that are connected to that profile. For example, the Author profile contains privileges specific to creating monitoring configurations.

MORE INFO USER ROLES

See <http://technet.microsoft.com/en-us/library/hh230728.aspx> for more information on implementation of user roles in Operations Manager.

Understanding self-service portal design using Service Manager

Maintaining an enterprise server infrastructure can be accomplished in a number of ways, but when considering management solutions that scale to large environments, the System Center 2012 R2 family of products comes to the forefront. For example, with Service Manager, you can create a self-service portal for end users, among other things. Service Manager provides incident and configuration management while enabling visibility into current issues. Service Manager uses a Configuration Management Database (CMDB) to provide a master location for all changes, issues, and requests for an infrastructure. Service Manager integrates with other System Center 2012 R2 products to provide an end-to-end solution.

At a minimum, there are three components to a Service Manager implementation: a management server, a configuration management database server, and the management console. Additional components can be added for things like data warehousing, which then facilitates reporting.

Using the self-service portal, users can find answers to common support questions, change their passwords, create help-desk tickets, and request software. When designing a management structure, you should consider deployment of the self-service portal to ease the burden on IT and the help desk for common requests. The end-user self-service portal requires a Silverlight component to run on the client computer and thus is applicable only to those platforms that can run Silverlight through the browser.

MORE INFO SELF-SERVICE PORTAL

See <http://technet.microsoft.com/library/hh667344.aspx> for more information on the self-service portal in Service Manager.

Delegating rights for the private cloud

System Center 2012 Virtual Machine Manager provides a centralized management console for virtual machines, such as those managed by Hyper-V. VMM manages virtual machines, networks, and storage as resources, which are then configured within the organization. A VMM deployment consists of a management server, database, library (and library server), and console.

Another component of managing the private cloud is App Controller. App Controller looks at service provision from a service-oriented view rather than from a server or software view. In other words, using App Controller you can connect the components that make up a service to facilitate management.

User roles can be created to manage various aspects of private cloud-based virtualization infrastructure. Virtual Machine Manager can be used to create such a delegation, and then App Controller can be used to manage the private cloud.

Rights are managed within the User Roles area of the Security section in the Settings area of Virtual Machine Manager. User roles can be created using individual user accounts or using Active Directory groups. The scope of the user role can then be assigned to the private cloud, as shown in Figure 1-2.

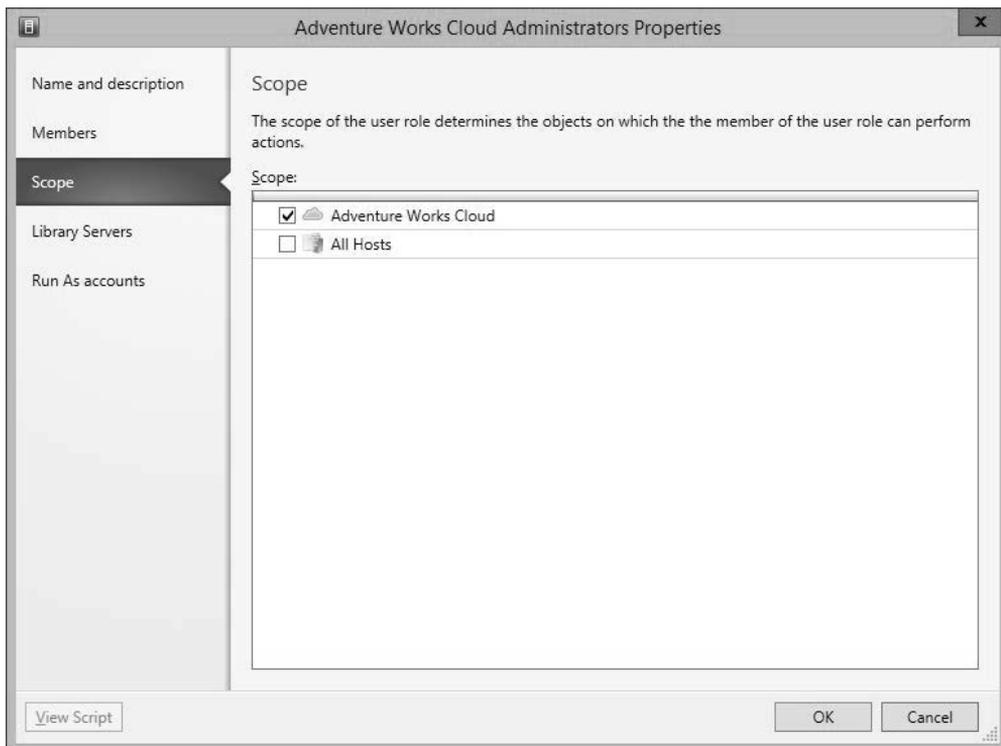


FIGURE 1-2 Assigning a scope to a user role for private clouds in Virtual Machine Manager

Members that have been assigned to the new user role will be able to log on to App Controller and manage private clouds within the user role scope.

An alternate method to assign access is by clicking Assign Cloud from the VMs and Services section in Virtual Machine Manager. Doing so enables you to select the user role to be assigned privileges for a given cloud or to create a new user role for the private cloud, as shown in Figure 1-3.

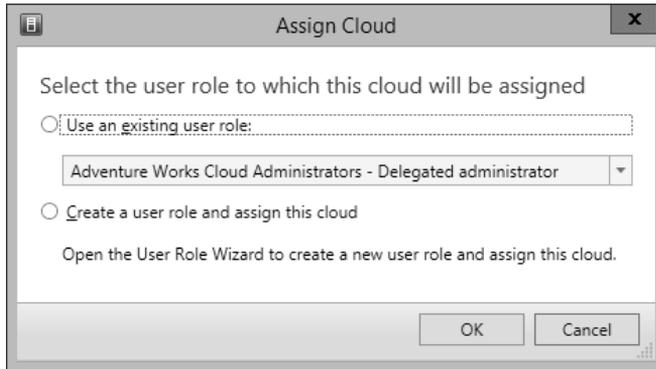


FIGURE 1-3 Assigning a user role to a cloud in the Assign Cloud dialog box

MORE INFO DELEGATING RIGHTS

See <http://technet.microsoft.com/en-us/library/hh221343.aspx> for more information on rights delegation.



Thought experiment

Delegating administrative authority

In the following thought experiment, apply what you've learned about this objective to predict what steps you need to take. You can find answers to these questions in the "Answers" section at the end of this chapter.

You're working on delegating administrative authority for your Configuration Manager deployment. You need to enable certain individuals to apply updates to test computers and, once tested, enable another set of individuals to apply those updates in the production environment.

Describe the overall concepts and types of configuration items that you'll use in Configuration Manager to facilitate this design.

Objective summary

- User rights and built-in groups can be used to provide a robust administrative model.
- Certain user rights shouldn't be assigned to users or groups but are instead used by system processes and functions.
- Built-in groups have certain user rights inherently assigned to them.
- System Center 2012 R2 can utilize a delegated administration structure that enables separation of responsibilities within an infrastructure.
- Security roles, security scopes, and collections are all used to facilitate the delegated administration structure necessary.
- Determining who, which and where, and what can be helpful for designing a delegation of role structure.
- Service Manager is used to provide end-user self service.
- Service Manager requires at least three servers to run including a management server, configuration management database server, and console.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Which of the following permissions allows the currently logged on user to shut the computer down?
 - A. SeShutdownComputer
 - B. SeShutdownPrivilege
 - C. SePrivilegeShutdown
 - D. En_ShutdownComputerPermission
2. Which of the following is not a privilege of the built-in Backup Operators group?
 - A. Shut down the system
 - B. Create symbolic links
 - C. Back up files and directories
 - D. Allow logon locally
3. Which of the following roles provides the core functionality for System Center?
 - A. Site server
 - B. Component server
 - C. Core server
 - D. Site Core server

4. Which of the following are not built-in security scopes in Configuration Manager?
- A. All
 - B. System
 - C. Administrator
 - D. Default

Objective 1.2: Design a monitoring strategy

As it pertains to the exam, Operations Manager is the primary tool used for enterprise monitoring. Operations Manager provides security logging (through Audit Collection Services) and performance monitoring and meets the criteria for centralized monitoring and reporting, which are all part of the objectives for this section.

This objective covers how to:

- Understand monitoring servers using Audit Collection Services (ACS) and System Center Global Service Monitor, performance monitoring, application monitoring, centralized monitoring, and centralized reporting
- Implement and optimize System Center 2012 R2 Operations Manager management packs
- Plan for monitoring Active Directory

Enabling Audit Collection Services (ACS)

Part of Operations Manager, Audit Collection Services (ACS) collects audit policy records for analysis and reporting. When used as part of an overall monitoring design strategy, ACS is responsible for collecting security-related events. This effectively means that you can gather security audit logs from multiple sources, including Linux and Unix-based computers, and access them from that centralized console for reporting and further action, as necessary.

ACS consists of the following:

- **ACS forwarders** The ACS forwarder is included, but not enabled, as part of the Operations Manager agent installation. Once enabled, security events are sent to the ACS collector and the local security event log.
- **ACS collector** The ACS collector is responsible for processing events from ACS forwarders so that the event can be entered into the database.
- **ACS database** The ACS database relies on SQL Server as its backend database and is responsible for holding the events sent to it from the ACS collector.

Each of these components can exist on the same server, though you'll install ACS forwarders on each computer to be monitored. When considering performance and as the deployment

grows, the collector and ACS database servers can be split onto separate servers. For many enterprise deployments, SQL Server will exist on a separate server as part of the initial rollout of Operations Manager.

MORE INFO ACS SYSTEM REQUIREMENTS

See <http://technet.microsoft.com/en-us/library/hh212908.aspx> for more information on ACS system requirements.

ACS forwarders are not enabled as part of the normal health-monitoring agent in Operators Manager. Instead, ACS forwarders are enabled through the Monitoring, Operations Manager, Agent Health State section of the Operations Manager console. Within the details pane of this area, selecting the computers (agents) and then selecting Enable Audit Collection within the Health Service Tasks section of the Actions pane enables ACS to begin collecting from that computer.



EXAM TIP

If necessary, a firewall exception for TCP port 51909 should be added to allow an ACS forwarder to communicate with the ACS collector.

When designing ACS-based solutions, the number of events sent by forwarders can overwhelm the ACS collector. Additionally, the ACS collector queues events when the ACS database server is offline, such as for maintenance. The collector queue has settings that can be adjusted for performance. These settings are in the registry at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AdtServer\Parameters. The settings are described in Table 1-9.

NOTE MANAGING DOWNTIME

The Enterprise version of SQL Server can be deployed to prevent maintenance-related downtime.

TABLE 1-9 ACS collector queue settings

Setting	Description	Default
MaximumQueueLength	The maximum number of events that can be held in the ACS collector queue if the database is offline.	0x40000
BackOffThreshold	The maximum number of queued events before the ACS collector denies new connections. The value is a percentage of the MaximumQueueLength.	75
DisconnectThreshold	The maximum number of queued events before the ACS collector begins disconnecting ACS forwarders. Like BackOffThreshold, this value is a percentage of the MaximumQueueLength.	90

ACS collects every Windows Security Event for each forwarder involved in the deployment. This can be a large amount of data and, in many instances, isn't necessary. One approach is to create a filter to prevent unnecessary events from being logged to the ACS database. Combining a filter with a policy for archiving ACS events ensures that compliance is met while at the same time not overwhelming the ACS implementation (or the administrators responsible for it).

Management of ACS is accomplished using the AdtAdmin.exe command-line tool found in %WINDIR%\System32\Security\AdtServer. Using AdtAdmin, you can create groups, show information about forwarders, and filter audit event data.

You might filter event data if the ACS collector queue is becoming full. ACS event filters are defined using Windows Management Instrumentation Query Language (WQL), which is a subset of standard SQL.

Table 1-10 describes some of the parameters available for AdtAdmin.

TABLE 1-10 AdtAdmin parameters

Parameter	Description
/AddGroup	Creates a group of ACS forwarders.
/DelGroup	Deletes a group of ACD forwarders.
/Disconnect	Disconnects an ACS forwarder or group.
/GetDBAuth	Shows information regarding the connection between the collector and database.
/GetQuery	Shows the current WQL queries being used by the ACS collector.
/ListForwarders	Shows information about forwarders.
/ListGroup	Shows the groups available on the collector.
/SetDBAuth	Sets the authentication method (SQL or Windows authentication) between the collector and the database.
/SetQuery	Configures a WQL query for filtering audit events.
/Stats	Shows statistics about the forwarders.
/UpdForwarder	Makes changes to a forwarder, including its name or the group to which the forwarder belongs.
/UpdGroup	Renames a group.

As described in Table 1-10, the current value of the WQL query can be obtained using the command:

```
AdtAdmin /getquery
```

By default, the WQL query for events is:

```
select * from AdtsEvent
```

MORE INFO ADTADMIN AND CHANGING THE DEFAULT QUERY

See <http://technet.microsoft.com/en-us/library/hh230740.aspx> for more information, including an example query for filtering events with WQL on ACS. See <http://technet.microsoft.com/en-us/library/hh212727.aspx> for additional information on AdtAdmin.exe.

The performance of ACS can be monitored through the Operations Manager console. Several counters are included by default and can be used to help diagnose and monitor performance of ACS itself.

MORE INFO ACS PERFORMANCE MONITORING

See <http://technet.microsoft.com/en-us/library/hh230714.aspx> for more information on performance counters for monitoring ACS performance.

Understanding Global Service Monitor

Global Service Monitor is provided as a management pack for Operations Manager and as part of an online offering such as a cloud-based service. Global Service Monitor provides an external view of websites for an organization. Global Service Monitor has two primary components: an online component managed by Microsoft and an Operations Manager component, which is handled as a management pack.

It's important to understand how Global Service Monitor fits within an enterprise scenario. Global Service Monitor is used for monitoring externally facing websites, such as those hosted through Microsoft Azure; as such, it fits within but isn't intended to be a replacement for Operations Manager but rather an enhancement to an Operations Manager installation. Global Service Monitor facilitates and makes easy the process of setting up multiple, globally dispersed monitoring locations for web applications.

The next section describes importing management packs as well as additional monitoring scenarios discussed in the objective domain for the 70-414 exam. Once a management pack is imported and a subscription started, you can configure monitoring through Operations Manager. Tests run with Global Service Monitor can be executed from multiple locations around the world so that you can have a complete view into your web application.

The simplest of tests is the Web Application Availability Monitoring test, which performs a basic HTTP request from an external location. If you need a more complex test, such as when you need to view multistep transactions or provide authentication details, then the Visual Studio Web Test Monitoring scenario is the correct choice. Finally, Web Application Transaction Monitoring provides monitoring for internal web applications that aren't available from external locations.

When configuring a test, you can set several parameters, such as the length of time that a request can take, the interval between requests, whether to look for specific text on the resulting page, and many additional settings, as shown in Figure 1-4.

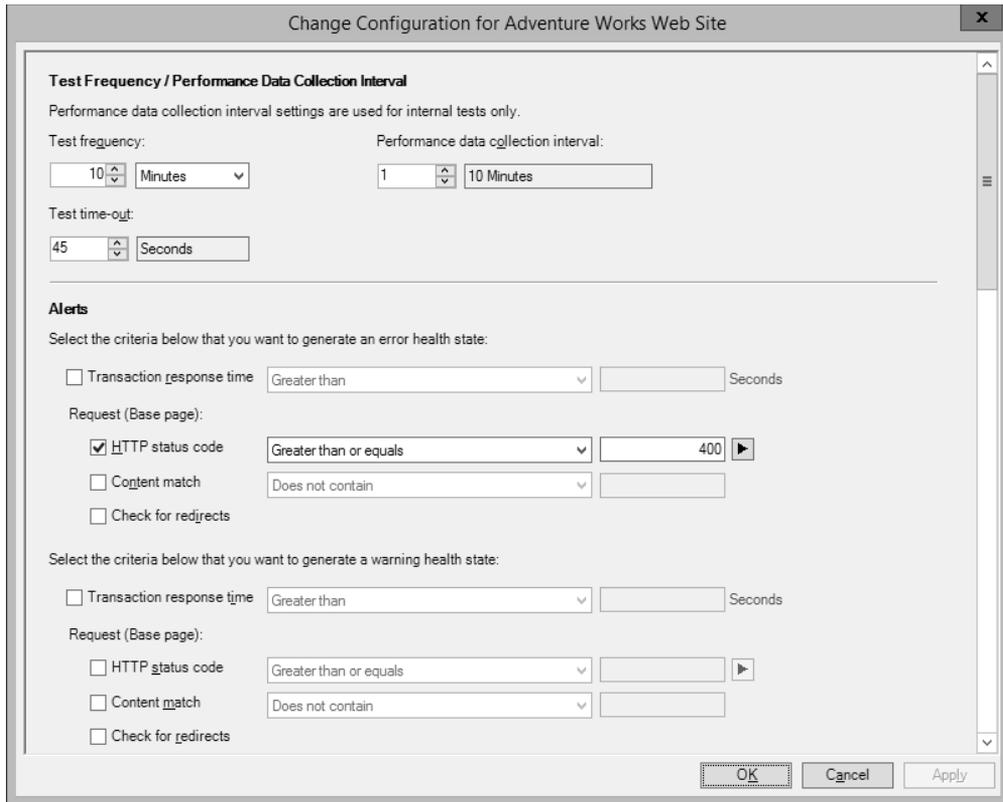


FIGURE 1-4 Configuring parameters related to a web availability test in Global Service Monitor

These settings are useful when you need to ensure specific behavior of a webpage or ensure that the page is served in less than a certain number of seconds. You can even check portions of the request, such as the time it takes to receive the first byte, the time it takes for DNS resolution, and so on.

When integrating Global Service Monitor into a monitoring design, consider the areas from which your customers will most likely access your website. Choose external monitoring locations close to your customer base.

MORE INFO CONFIGURING GLOBAL SERVICE MONITOR

Because this is a design-based objective, the actual configuration steps aren't covered in this text. Instead, see <http://technet.microsoft.com/en-us/library/jj860370.aspx> and <http://technet.microsoft.com/en-us/library/jj860376.aspx> for specific information on configuration in Global Service Monitor.

Implementing and optimizing Operations Manager management packs

Looking beyond performance monitoring of ACS, Operations Manager can provide performance monitoring, application monitoring, and reporting for Windows computers and the network as a whole. To do so, a System Center management pack can be installed. The management pack contains additional information about monitoring points for Windows Server.

Management packs provide information about how to monitor servers, applications, and services on a network. Management packs can also provide reports, tasks, and other components as defined by the management pack. For example, a management pack for a Windows Server might contain information on how to monitor disk performance. Management packs can be created by third parties to provide an integrated monitoring solution within Operations Manager.

MORE INFO MANAGEMENT PACKS

If you're unfamiliar with management packs, see "What Is in an Operations Manager Management Pack?" at <http://technet.microsoft.com/en-us/library/hh212794.aspx> for additional details.

The management pack lifecycle includes the following stages:

- Install the management pack in a nonproduction environment to ensure that the management pack is compatible and provides the desired functionality.
- Customize the management pack. Create overrides, add knowledge, and make other changes to the management pack for your environment.
- Deploy the management pack. Install the management pack and any changes in the production environment.
- Maintain the management pack. As your environment changes, you may need to make changes to the management pack. For example, you may require additional monitoring, or the application being monitored may change.

IMPLEMENTING A MANAGEMENT PACK

Management packs are added through the Administration area of the Operations Manager console by clicking Import Management Packs. The Import Management Packs Wizard will begin and enable you to choose the location from which the management pack should be installed. You can choose an existing catalog or add from a file. Alternately, the Import-SCOMManagementPack cmdlet is used to import a management pack using Windows PowerShell.

MORE INFO IMPORTING MANAGEMENT PACKS

Importing management packs is covered in depth at <http://technet.microsoft.com/en-us/library/hh212691.aspx>.

Monitoring Windows servers requires the Windows Server Operating System Library, the Windows Server 2012 Operating System (Discovery), and the Windows Server 2012 Operating System (Monitoring) management packs. The Import Management Packs tool, shown in Figure 1-5, can resolve dependencies. For example, selecting the Windows Server 2012 Operating System (Monitoring) management pack requires that the additional management packs mentioned earlier be installed as well. The Import Management Packs tool can install those prerequisites.

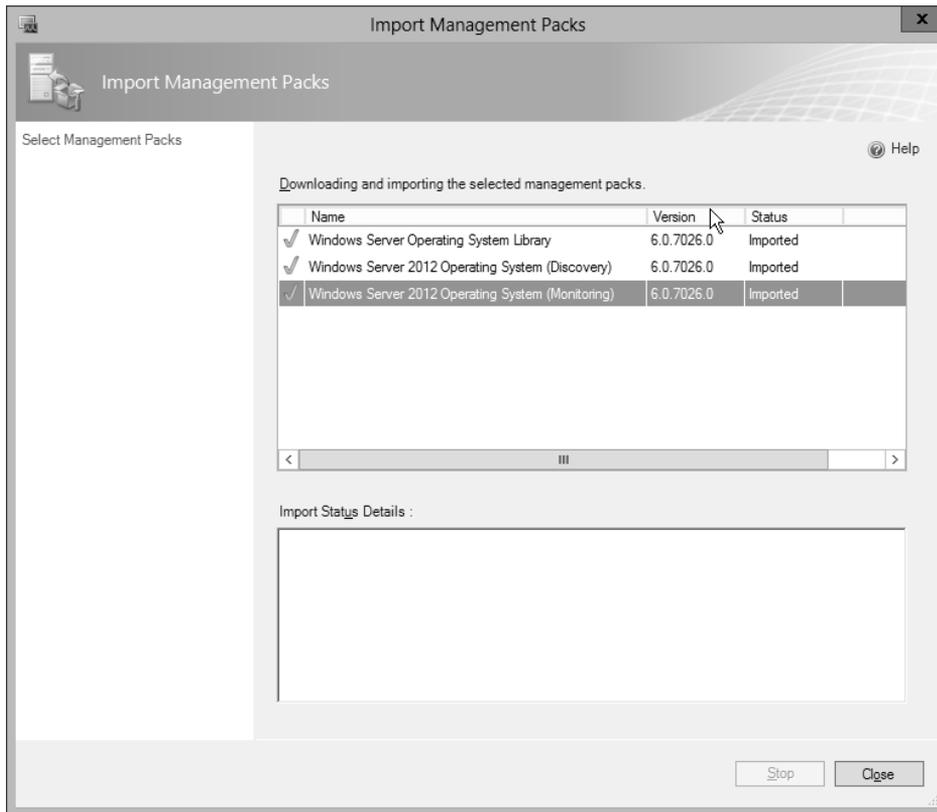


FIGURE 1-5 Importing a management pack with dependencies

MANAGEMENT PACK OPTIMIZATION

An important step in deploying management packs is optimizing them for your environment. When first installed, management packs perform discovery to find applicable objects for monitoring. Those objects are then monitored according to the rules set forth in the

management pack. The default management pack rules may not be appropriate for your environment and should therefore be changed as necessary.

NOTE CREATE A NEW MANAGEMENT PACK

When making changes to a management pack, it is recommended that you create a new management pack for the changes, rather than changing the default.

The overall process for optimizing a management pack is to examine the highest severity alerts first and then proceed to the lowest severity. Alerts should be examined to ensure that they are both valid and actionable. In other words, if you don't need to react when an event occurs, then it's probably not worth alerting. That's not to say that the event isn't noteworthy, so it may need to be logged but not alerted. Related to alerting is ensuring that only one alert is generated for a given event.

Management packs are customized through overrides. Overrides change the configuration of a monitor or diagnostic. When configuring an override, you choose whether the override will apply to all objects of the current class (such as all Windows Server 2012 computers), to a group, to a specific object of the current class, or to all objects of another class. This gives you the flexibility to gather objects for which you don't need alerts, such as nonproduction Windows servers.

Classes, sometimes called *targets*, are used to help define the items that can be discovered and managed. Groups are sets of objects that help define the scope of an override.

NOTE CLASSES AND GROUPS

Classes can be applied for monitors, rules, discoveries, overrides, and tasks. Groups can define scope for overrides, views, user roles, and notifications.

MORE INFO USING CLASSES AND GROUPS

See <http://technet.microsoft.com/en-us/library/hh212771.aspx> for more information on classes and groups for overrides, and see <http://technet.microsoft.com/en-us/library/hh212869.aspx> for information on creating an override.

Another optimization for management packs is achieved through knowledge. Knowledge is used to provide notes and other information about a monitor or rule. Adding knowledge is accomplished in the Authoring workspace of the Operations Manager console within the properties settings for a given monitor or rule. However, as of this writing, adding or editing knowledge requires the Operations Manager console on a 32-bit operating system with the 32-bit version of Microsoft Word 2010 and other prerequisites as described at <http://technet.microsoft.com/en-us/library/hh212900.aspx>. Adding or editing knowledge requires the Author or Administrator role.

Planning for Active Directory monitoring

The AD DS management pack for System Center enables monitoring of several aspects of an AD DS environment. Several key monitoring scenarios for Active Directory monitoring are identified at <http://technet.microsoft.com/library/dd262116.aspx> and described in Table 1-11.

TABLE 1-11 Active Directory monitoring scenarios

Scenario	Description
Multi-forest monitoring	Gather health and performance data from remote forests through two workflows, Microsoft.AD.Topology.Discovery and Microsoft.AD.Remote.Topology.Discovery. Note that AgentProxySetting must be enabled on all domain controllers for this scenario.
Replication	Gather health of data replication between domain controllers. You can monitor both health and performance of replication. See http://technet.microsoft.com/en-us/library/dd262066.aspx and http://technet.microsoft.com/en-us/library/ee662305.aspx for more information on each of these aspects of replication monitoring.
Essential services	Gather health information on the following services, which are vital to the operation of Active Directory: NT File Replication Service (NTFRS) Distributed File System Replication (DFSR) Windows Time Service (W32Time) Intersite Messaging (ISM) Key Distribution Center (KDC) NT Directory Services (NTDS) Net Logon (NetLogon) Active Directory Web Service (ADWS)
Trust monitoring	Gather trust information using the TrustMon WMI provider.
Directory service availability	Gather various metrics on the availability of Active Directory, including: GC Response - The time it takes to load the global catalog GC Search Time - The time it takes to return a search result from a global catalog Lost & Found Count - The number of Lost and Found objects DNS Verification - Verify DNS records AD General Response - The time it takes to do a serverless bind
Active Directory database monitoring	Verify the health of the Active Directory database, including its size, consistency, and that there is sufficient space available for the database to grow.
Time skew monitoring	Gather information on the time skew or difference between computers taking part in authentication. The authoritative time source is chosen as follows: The primary domain control (PDC) for the root domain is authoritative in all instances. If a computer is a PDC for a nonroot domain, the PDC for the root domain is authoritative. If a computer is not a PDC then its own local PDC is authoritative.
Operations Master monitoring	Gather information on availability of the following Operations Master roles: Schema Operations Master Domain Naming Operations Master Infrastructure Operations Master Relative ID (RID) Operations Master PDC Emulator Operations Master



Thought experiment

Managing Active Directory performance

In the following thought experiment, apply what you've learned about this objective to predict what steps you need to take. You can find answers to these questions in the "Answers" section at the end of this chapter.

You've set up the Active Directory management pack. After receiving reports of slow logons, you investigate.

- 1.** What are some of the performance indicators and alerts you can examine?
- 2.** Where are those performance indicators and alerts located?

Objective summary

- Management packs are configured using overrides, which include customizations for your infrastructure.
- ACS is composed of one or more forwarders, an ACS collector, and an ACS database.
- The AdtAdmin.exe program can be used to configure ACS.
- The Active Directory management pack enables advanced performance monitoring and alerting for an Active Directory domain.
- Global Service Manager provides an external view of web application performance from multiple geographically dispersed locations.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

- 1.** Which of the following commands would be used to change the audit event filter for ACS?
 - A.** AdtAdmin /setquery
 - B.** AdtAdmin /addFilter
 - C.** AcsAdmin /addFilter
 - D.** AcsFilter /add

2. Which of the following roles is required to add or edit company knowledge for a management pack?
 - A. Operator
 - B. Knowledge Administrator
 - C. Author
 - D. Management Pack Administrator

3. Which of the following is not an essential service for Active Directory monitoring?
 - A. NTDS
 - B. NetLogon
 - C. DFSR
 - D. ADMon

4. What is the correct registry path for collector queue settings?
 - A. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ADT \Parameters
 - B. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AdtServer\Parameters
 - C. HKEY_LOCAL_MACHINE\User\CurrentWindowsServices\AdtServer\Parameters
 - D. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AdtSvc\Parameters

Objective 1.3: Plan and implement automated remediation

This objective covers how to:

- Create an update baseline in Virtual Machine Manager
- Implement a Desired Configuration Management (DCM) baseline
- Implement Virtual Machine Manager integration with Operations Manager
- Configure Virtual Machine Manager to move a VM dynamically based on policy
- Integrate System Center 2012 R2 for automatic remediation into your existing enterprise infrastructure
- Design and implement a Windows PowerShell Desired State Configuration (DSC) solution

Creating an update baseline in VMM

Update baselines are used to manage updates within a VMM fabric. For example, a virtual machine can be compared to the update baseline and, if found to be out of compliance with that baseline, the virtual machine can be remediated and brought into compliance.

When VMM is configured with a WSUS server and synchronization is complete, two sample update baselines will be created. These samples can be found within the Update Catalog And Baselines area of the Library workspace, shown in Figure 1-6.

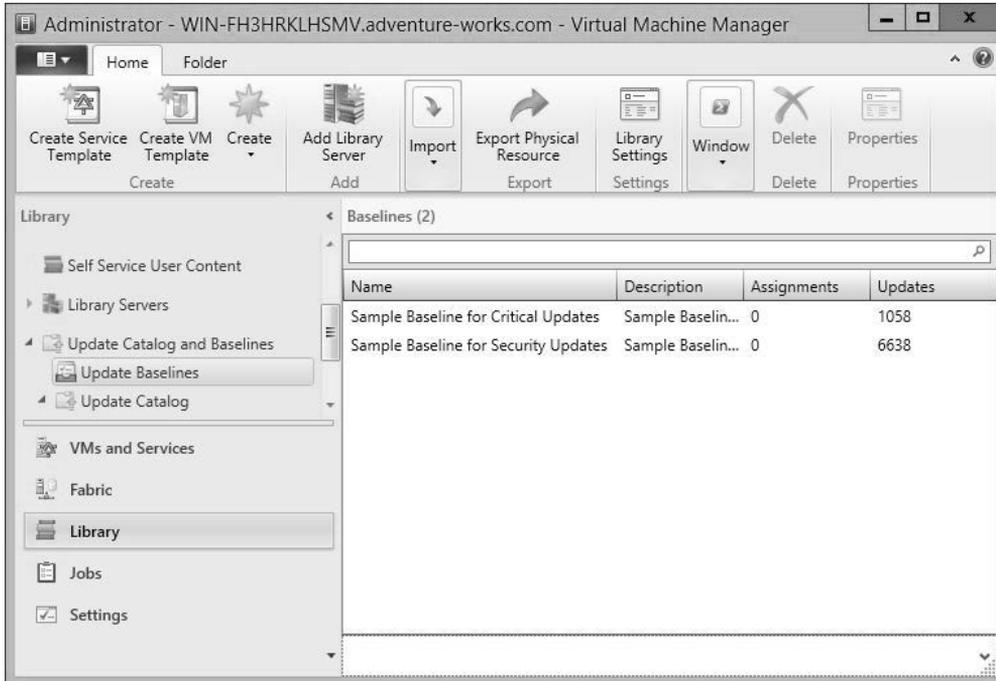


FIGURE 1-6 Sample baselines in VMM

When working with baselines, you can use one of the existing sample baselines or create a new one. This section looks at creating a new baseline in VMM.

An update baseline is created in the Update Baselines area of the Library workspace. Within that area, selecting Baseline from the Create group opens the Update Baseline Wizard. In the Update Baseline Wizard, you first specify a name and optionally a description, as shown in Figure 1-7.

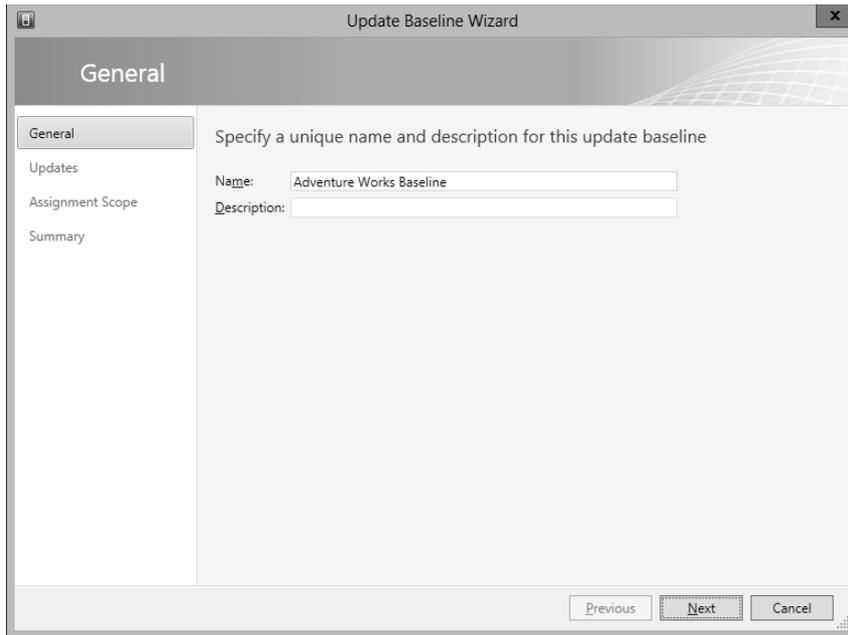


FIGURE 1-7 Entering a name to create a new baseline

Next, you select the updates that will be included in this baseline. For this example, a single update has been selected, as shown in Figure 1-8, but you could select more updates by clicking Add.

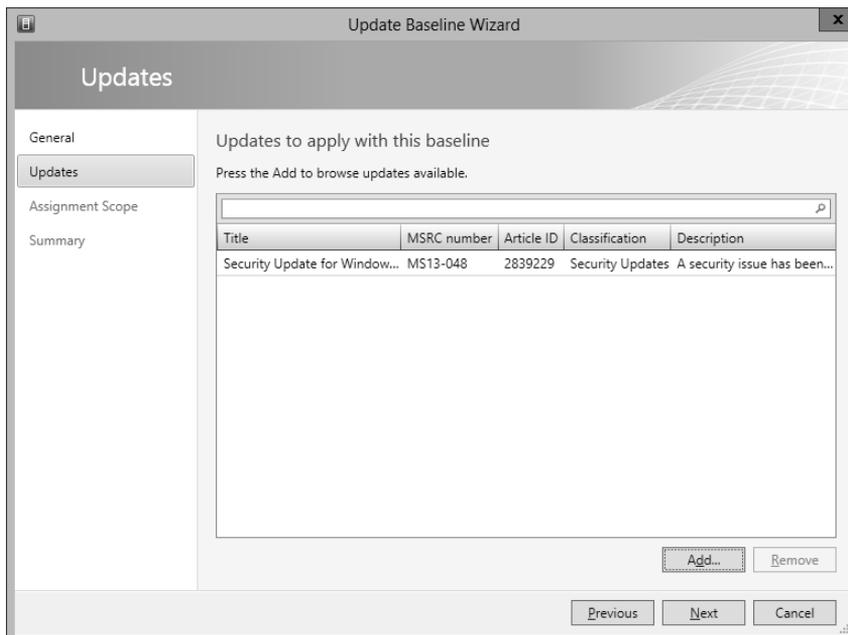


FIGURE 1-8 Selecting updates for the baseline

Finally, you select the scope to which the baseline will apply. This is accomplished within the Assignment Scope page, shown in Figure 1-9, where All Hosts has been selected.

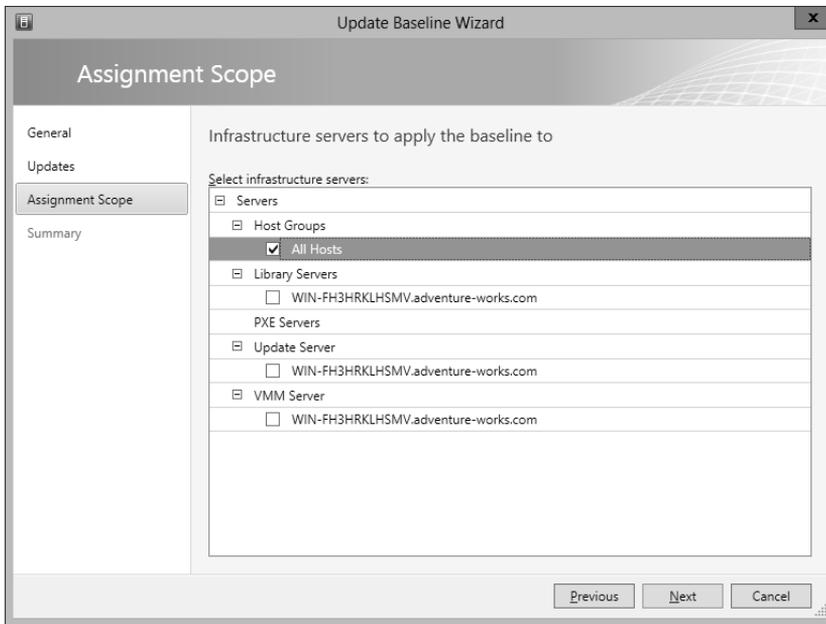


FIGURE 1-9 Choosing an assignment scope

Once complete, the summary page will display, and clicking Finish will start the jobs for baseline creation. The newly created baseline will be shown in the VMM console, as depicted in Figure 1-10.

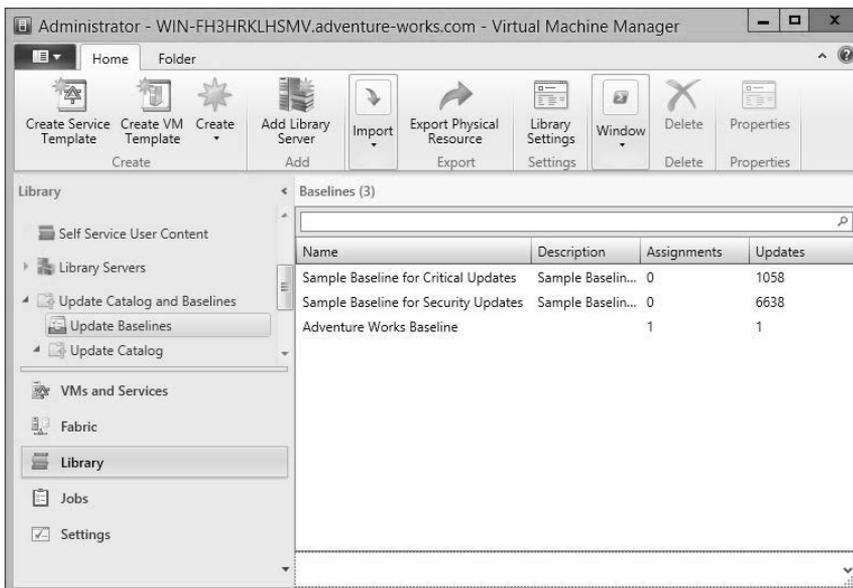


FIGURE 1-10 The newly created update baseline

You also have the option to create a baseline using Windows PowerShell. The relevant cmdlets include:

- **New-SCBaseline** Creates the new baseline and assigns it a name and a description
- **Set-SCBaseline** Changes parameters such as the host group and update list to the baseline

When using the Update Baseline Wizard, the final step enables you to view the scripts that will be run as part of the VMM job. The script that was executed to create the Adventure Works Baseline example is shown here:

```
$baseline = New-SCBaseline -Name "Adventure Works Baseline" -Description ""
$addedUpdateList = @(
$addedUpdateList += Get-SCUpdate -ID "7254a3fc-98db-4ca6-ad3f-3bf095de0bc8"
$scope = Get-SCVMHostGroup -Name "All Hosts" -ID "0e3ba228-a059-46be-aa41-2f5cf0f4b96e"
Set-SCBaseline -Baseline $baseline -AddAssignmentScope $scope -JobGroup
"c1477221-a4a0-4c4f-82ef-e502b46a517f" -RunAsynchronously
Set-SCBaseline -Baseline $baseline -RunAsynchronously -AddUpdates $addedUpdateList
-JobGroup
"c1477221-a4a0-4c4f-82ef-e502b46a517f" -StartNow
```

MORE INFO UPDATE BASELINES

See <http://technet.microsoft.com/library/gg675110.aspx> for more information on creating update baselines in VMM.

Implementing a Desired Configuration Management (DCM) baseline and automatic remediation

DCM baselines are used in Configuration Manager to ensure compliance for a variety of configuration settings. This section focuses primarily on the exam objective of implementing DCM. DCM provides assessment of managed computers against desired or known-good configurations, for example, whether an update has been applied. This section looks at both the implementing DCM subobjective as well as the automatic remediation subobjective contained within the overall "Implement Automated Remediation" exam objective.

MORE INFO UNDERSTANDING DCM

See <http://technet.microsoft.com/en-us/library/bb680553.aspx> for an overview of DCM.

DCM baselines are configured within the Assets and Compliance workspace within Compliance Settings, Configuration Baselines. Clicking Create Configuration Baseline opens the Create Configuration Baseline dialog box. Within the Create Configuration Baseline dialog box, you enter details of the baseline to be created, as shown in Figure 1-11.

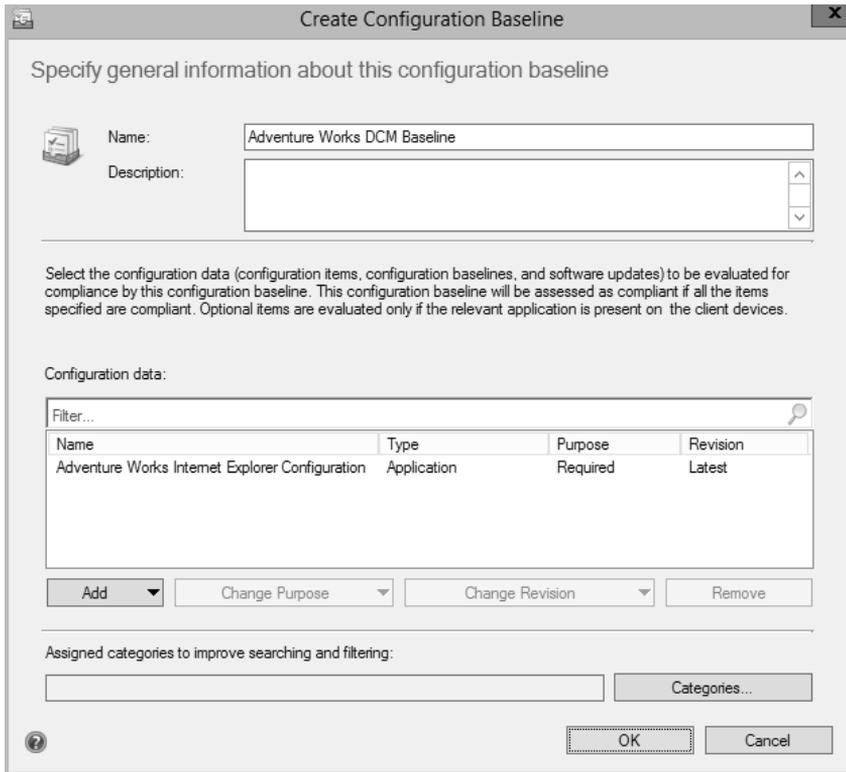


FIGURE 1-11 Creating a desired configuration baseline

A configuration baseline applies one or more configuration items, other configuration baselines, or software updates. The example shown in Figure 1-11 uses a previously defined configuration item, which was added through the Configuration Items page of the Compliance Settings area in Configuration Manager.

Once a configuration baseline is created, it needs to be deployed. This is accomplished by selecting Deploy within the Configuration Baselines area. Clicking Deploy opens the Deploy Configuration Baselines dialog box shown in Figure 1-12. You can select the Remediate Noncompliant Rules When Supported option, select the Generate An Alert option, and specify a schedule for the baseline to be deployed. The deployment will apply to the collection that you select within this dialog box.

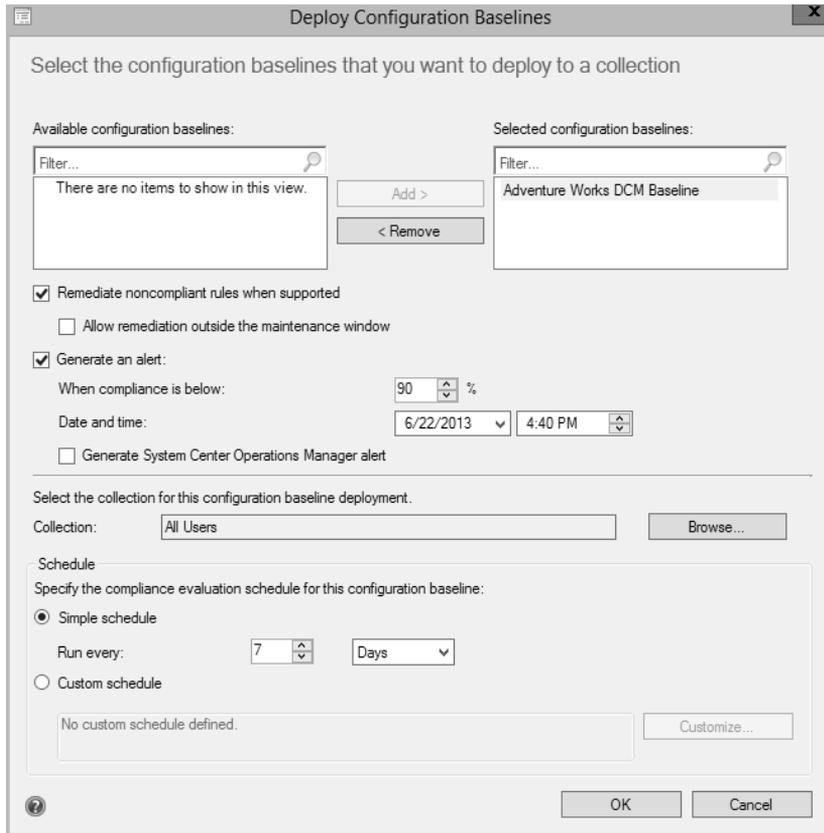


FIGURE 1-12 Preparing to deploy a configuration baseline

In addition to configuring automatic remediation through host groups, you can also configure automatic remediation within a configuration item or within the deployment of a configuration baseline. For example, Figure 1-13 shows the Edit Rule dialog box for a configuration item on the Compliance Rules tab. Note the Remediate Noncompliant Rules When Supported option is selected.

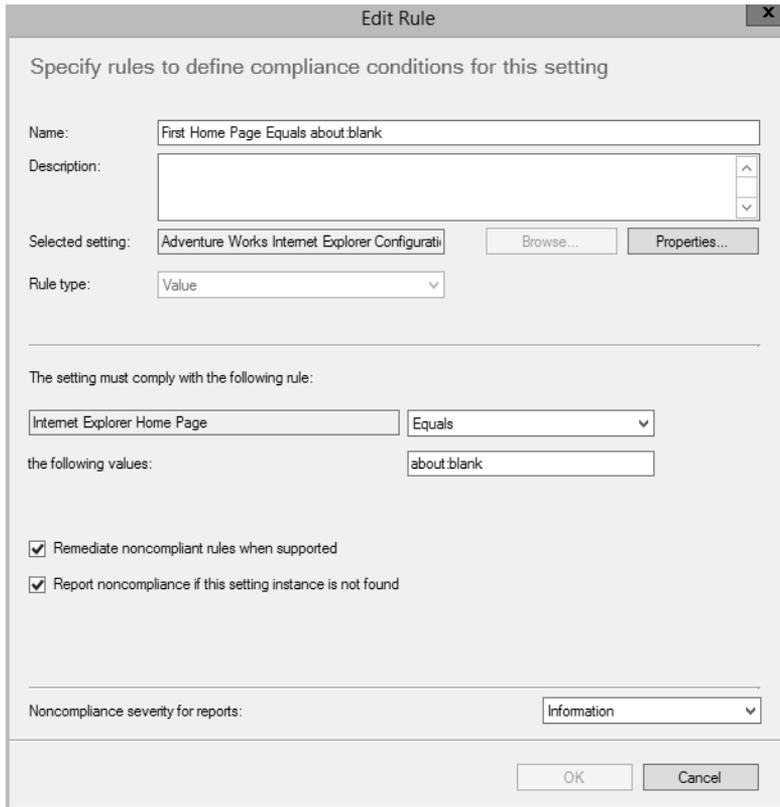


FIGURE 1-13 Editing a compliance rule of a configuration item

Implementing VMM integration with Operations Manager

Virtual Machine Manager can be integrated with Operations Manager. Integrating VMM and Operations Manager involves configuring both the Operations Manager server and the server running VMM.



EXAM TIP

Windows PowerShell 2.0 is required for System Center 2012, and Windows PowerShell 3.0 is required for System Center 2012 SP1 and System Center 2012 R2.

The first step in integration is to install the Operations Manager console on the VMM server. This is accomplished by using the Operations Manager Setup Wizard and selecting the Operations Manager console as the component to be installed.

MORE INFO INSTALLING THE OPERATIONS MANAGER CONSOLE

See <http://technet.microsoft.com/en-us/library/hh298607.aspx> for information on installing the Operations Manager console.

The next step in integrating VMM and Operations Manager is to install the agent on the server running VMM and on any virtual machines under its control. Many times this step has already been done as part of the Operations Manager rollout. However, if the Operations Manager agent hasn't yet been installed, do so as part of the integration implementation.

The Operations Manager agent can be installed manually or through an automated means, such as the native Operations Manager discovery process. Once installed, you should verify that the VMM server and its virtual machines can be seen from within the Operations Manager console.

MORE INFO INSTALLING THE OPERATIONS MANAGER AGENT

See <http://technet.microsoft.com/en-us/library/hh551142.aspx> for more information on methods to install the Operations Manager agent.

The next installation-related step is to import the appropriate management packs into Operations Manager. The necessary management packs include:

- Windows Server Internet Information Services 2003
- Windows Server 2008 Internet Information Services 7, including Windows Server 2008 Operating System (Discovery) and the Windows Server Operating System Library, which are prerequisites
- Windows Server Internet Information Services Library
- SQL Server Core Library

NOTE ABOUT THE PREREQUISITES

These seemingly outdated prerequisites are still necessary even though the Operations Manager and VMM servers are running Windows Server 2012 with Internet Information Services 8.0.

Integration of VMM and Operations Manager is accomplished from the VMM server, specifically in the Settings workspace of the VMM console. Within the Settings workspace, selecting System Center Settings reveals the Operations Manager Server, as shown in Figure 1-14.

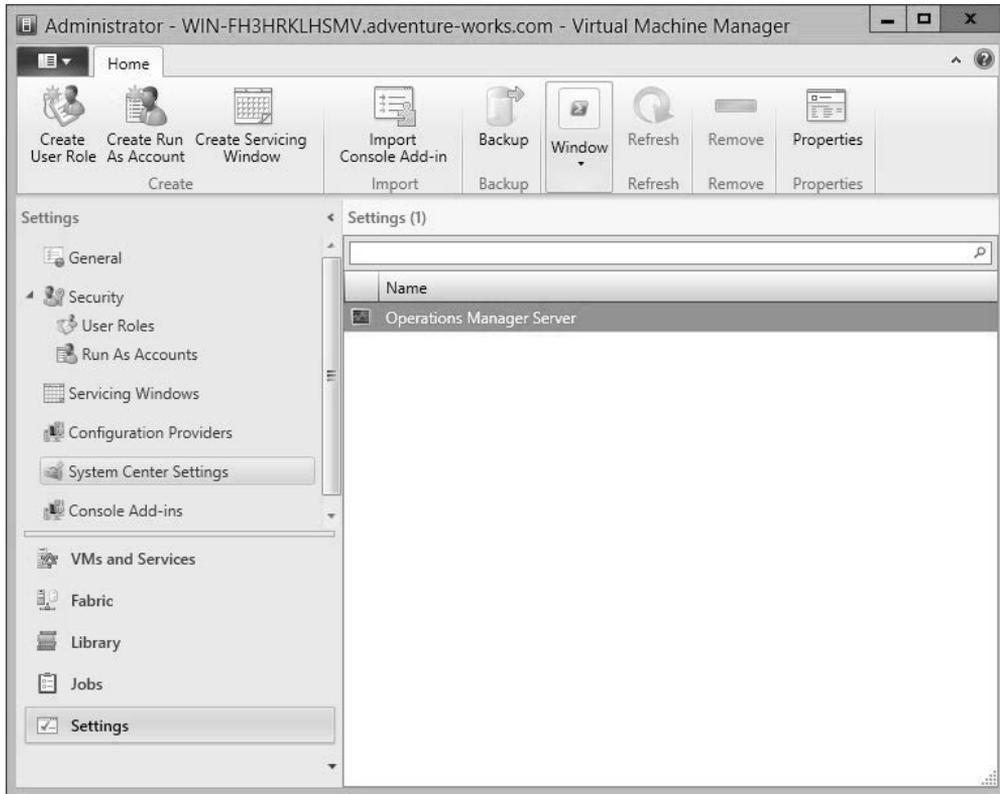


FIGURE 1-14 Viewing System Center settings

With Operations Manager Server selected, click Properties to start the Add Operations Manager Wizard, shown in Figure 1-15.

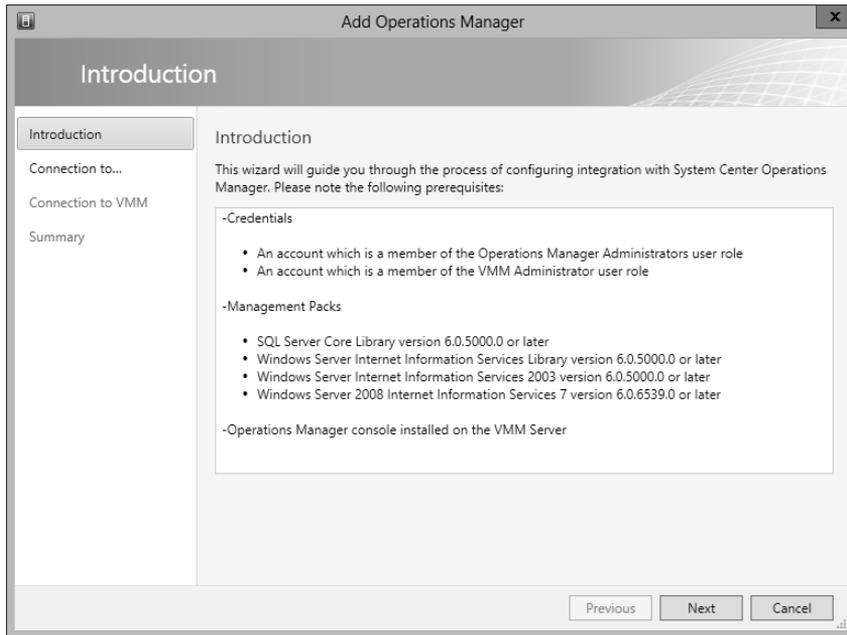


FIGURE 1-15 The Add Operations Manager Wizard

The Connection to Operations Manager page, shown in Figure 1-16, enables you to enter the server name and credentials, and to select the Enable Performance And Resource Optimization (PRO) and Enable Maintenance Mode Integration With Operations Manager options.

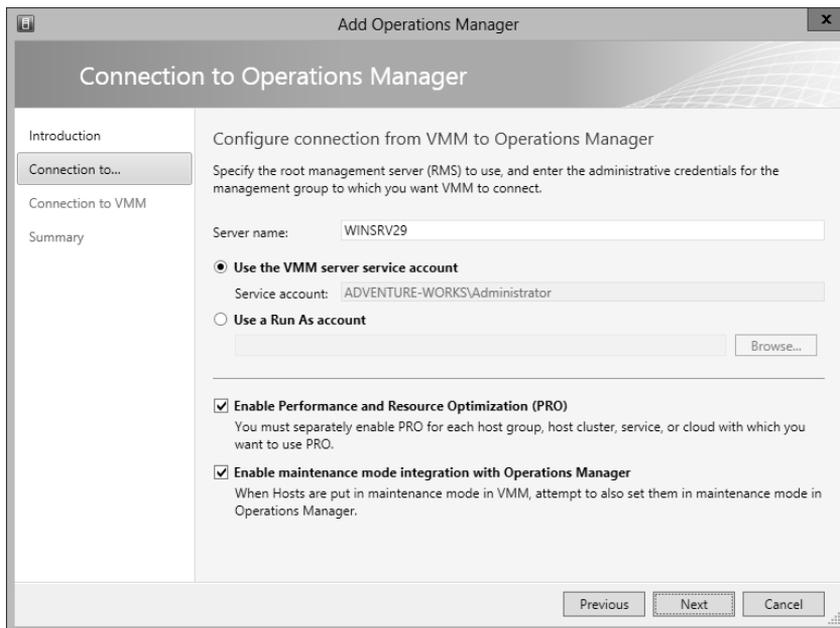


FIGURE 1-16 Adding details of the integration

The Connection to VMM page, shown in Figure 1-17, is where you specify credentials to be used by Operations Manager when connecting to VMM.

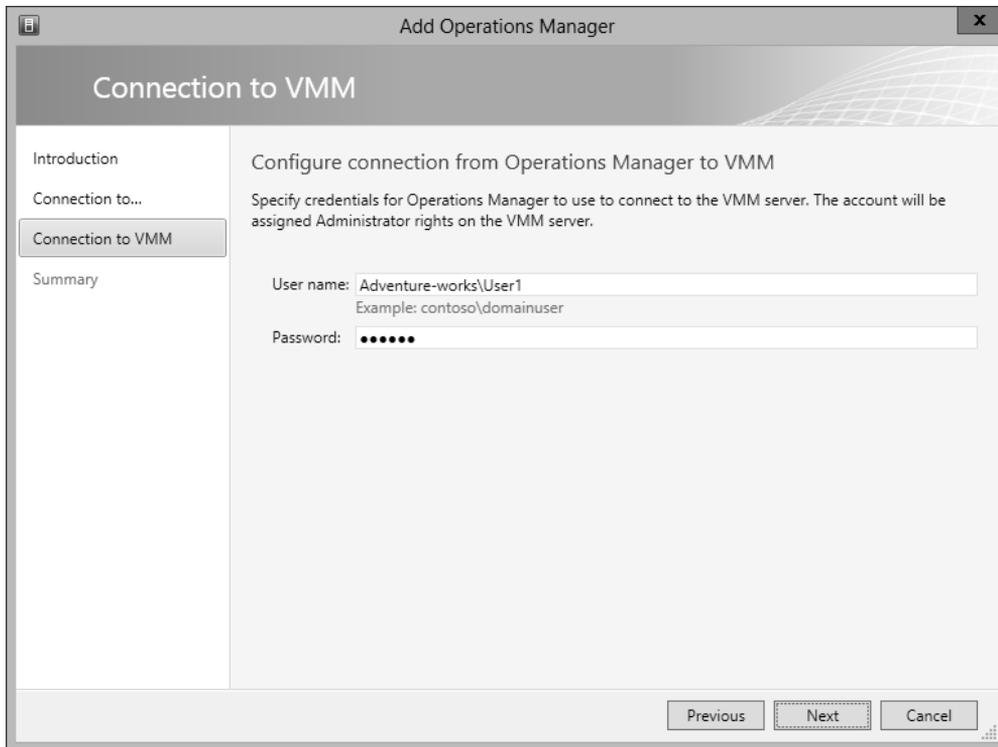
The image shows a screenshot of a Windows wizard window titled "Add Operations Manager". The window has a sidebar on the left with four steps: "Introduction", "Connection to...", "Connection to VMM" (which is selected and highlighted), and "Summary". The main area of the window is titled "Connection to VMM" and contains the following text: "Configure connection from Operations Manager to VMM" and "Specify credentials for Operations Manager to use to connect to the VMM server. The account will be assigned Administrator rights on the VMM server." Below this text are two input fields: "User name:" with the text "Adventure-works\User1" and "Example: contoso\domainuser" below it, and "Password:" with a masked password of seven dots. At the bottom right of the window are three buttons: "Previous", "Next" (which is highlighted with a dashed border), and "Cancel".

FIGURE 1-17 Specifying Operations Manager credentials

A summary page shows a summary of the configuration about to take place. When you click Finish, a job will begin the integration by installing the VMM management pack on the Operations Manager server.

Like other operations, integrating with Operations Manager can be accomplished through PowerShell. The `New-SCOpsMgrConnection` cmdlet can be used to add the connection.

MORE INFO THE NEW-SCOPSMGRCONNECTION CMDLET

See <http://technet.microsoft.com/en-us/library/hh801397.aspx> for more information on the `New-SCOpsMgrConnection` cmdlet.

Configuring VMM to move a virtual machine dynamically based on policy

This section provides a brief overview of automated migration of virtual machines using dynamic optimization.

Dynamic optimization enables virtual machines to be migrated between hosts in a host group based on load and other factors. Figure 1-18 shows the Dynamic Optimization page for a host group.

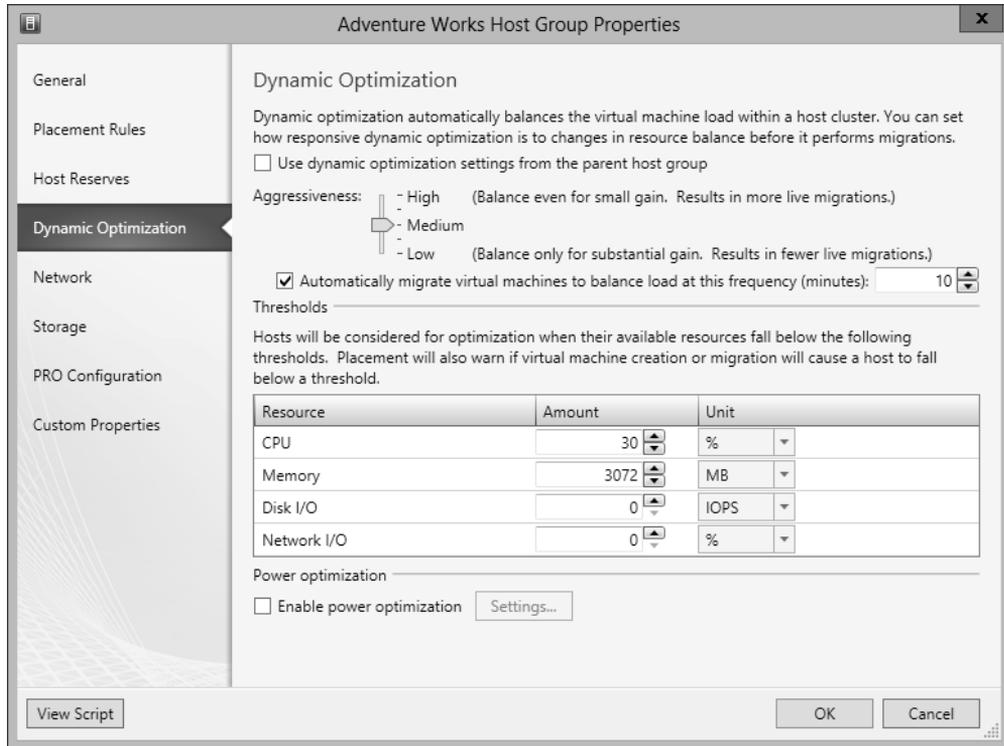


FIGURE 1-18 Configuring dynamic optimization in Virtual Machine Manager

By default, dynamic optimization rules will be inherited from the parent host group. (This option is not selected in Figure 1-18 to better illustrate the available options.) Dynamic optimization can be configured for manual migrations or automatic, as is depicted in Figure 1-18. Manual migrations are the default option, but when configured for automatic migrations, 10 minutes is the default frequency for dynamic optimization.

MORE INFO DYNAMIC OPTIMIZATION

See <http://technet.microsoft.com/en-us/library/gg675109.aspx> for more information on dynamic optimization.

Designing and implementing a Windows PowerShell Desired State Configuration solution

Desired State Configuration (DSC) is a new feature found in Windows PowerShell that enables scripting of configuration data. This configuration data can then be shared across servers to ensure consistency and promote ease of administration. For example, with DSC you can create a script that assists in deployment of web servers or other servers within the organization.



EXAM TIP

DSC is new with Windows Server 2012 R2.

The DSC service enables a server to act as a centralized repository for configuration scripts. When designing a DSC implementation for the enterprise, consider placing the DSC service server geographically close to the computers that will pull from it. Even though the configuration scripts themselves are small, you can store additional resources on the DSC service server, which could place a measurable load on resources.

DSC scripts are defined with the Configuration keyword and frequently written using Windows PowerShell Integrated Scripting Environment (ISE), as shown in Figure 1-19.

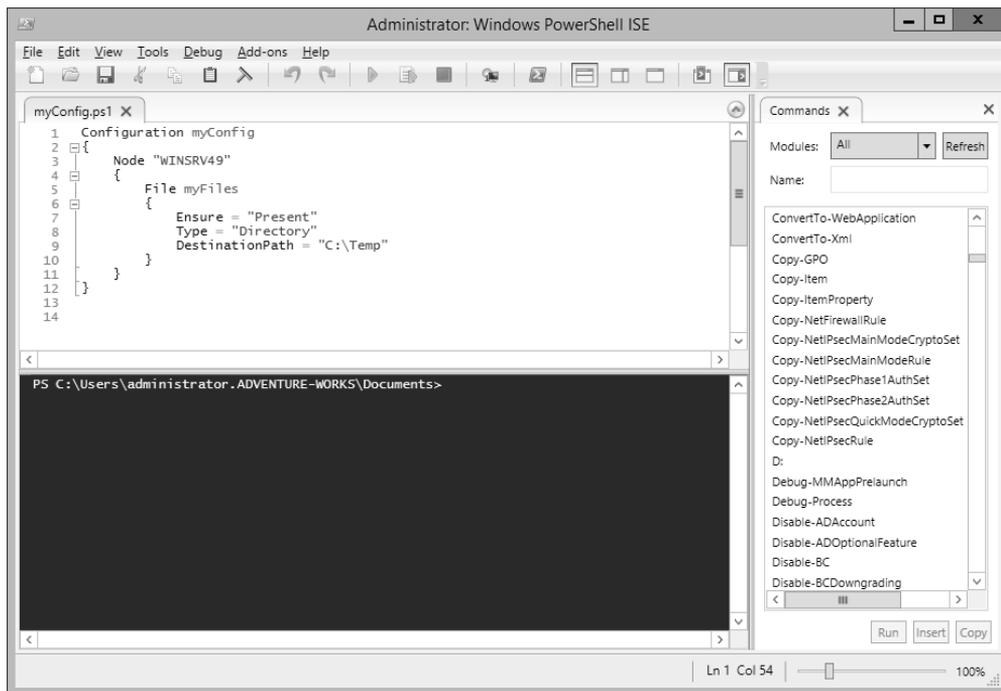


FIGURE 1-19 Creating a DSC script in Windows PowerShell ISE

Once created, the script is run from within the ISE and then enacted from within the ISE command prompt by typing the script name. Doing so creates Microsoft Operations Framework (MOF) files for each node identified in the script. For example, the following script (also shown in Figure 1-19) ensures that there's a directory called C:\Temp on the server named WINSRV49.

```
Configuration myConfig
{
    Node "WINSRV49"
    {
        File myFiles
        {
            Ensure = "Present"
            Type = "Directory"
            DestinationPath = "C:\Temp"
        }
    }
}
```

The MOF file is placed within a directory with the same name as the configuration script. From there, the desired configuration for a configuration named myConfig would be invoked with the command `Start-DscConfiguration -Wait -Verbose -Path .\myConfig`.

Once invoked, the command will run and apply the desired configuration to each of the servers (nodes) defined in the Configuration block.



EXAM TIP

You can also check to ensure that configuration changes are still applied to a given node using the `Test-DscConfiguration` cmdlet.

Parameters can be used within DSC scripts. Therefore, rather than repeating the same configuration within several hundred node blocks, you could instead use a parameter to define node programmatically, as shown here:

```
Configuration myConfig
{
    param ($nodeName)
    Node $nodeName
    {
        File myFiles
        {
            Ensure = "Present"
            Type = "Directory"
            DestinationPath = "C:\Temp"
        }
    }
}
```

MORE INFO DESIRED STATE CONFIGURATION

See <http://technet.microsoft.com/en-us/library/dn249918.aspx> for more information on getting started with DSC.



Thought experiment

Understanding update baselines

In the following thought experiment, apply what you've learned about this objective to predict what steps you need to take. You can find answers to these questions in the "Answers" section at the end of this chapter.

The infrastructure at your organization has shown remarkable growth over the past year. Unfortunately, the staff to maintain that infrastructure has not grown. Therefore, you're looking at ways to automate as many tasks as possible. You've been asked to brief the management team on some of the solutions available for automating the infrastructure.

- Describe update baselines and Desired Configuration Management.

Objective summary

- Update baselines provide an automated means by which virtual machines in a VMM deployment can have updates deployed automatically.
- DCM enables advanced configuration settings to be deployed across clients managed by Configuration Manager.
- System Center can be integrated for automatic remediation of various issues.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Which command creates an update baseline in VMM?
 - A. New-SCBaseline
 - B. Create-SCBaseline
 - C. SCBaseline /new
 - D. New-VMMBaseline

2. Which of the following is not a setting that can be used when creating a configuration management baseline?
 - A. Configuration Item
 - B. Software Update
 - C. Configuration Agent
 - D. Configuration Baseline

3. What's the default frequency for automatic dynamic optimization?
 - A. One day
 - B. One hour
 - C. 10 minutes
 - D. 24 hours

Answers

This section contains the solutions to the thought experiments and answers to the lesson review questions in this chapter.

Objective 1.1: Thought experiment

You'll likely use security roles to enable the administrators to apply those updates to a security scope of each type of server, test, and production. The key elements for this answer are the security roles and the security scopes.

Objective 1.1: Review

1. **Correct answer:** B
 - A. **Incorrect:** SeShutdownComputer is not a valid privilege.
 - B. **Correct:** SeShutdownPrivilege is the correct privilege.
 - C. **Incorrect:** SePrivilegeShutdown is not a valid privilege.
 - D. **Incorrect:** En_ShutdownComputerPermission is not a valid privilege.
2. **Correct answer:** B
 - A. **Incorrect:** Shut down the system is a privilege for the Backup Operators group.
 - B. **Correct:** Create symbolic links is not a privilege of the Backup Operators group.
 - C. **Incorrect:** Back up files and directories is a privilege for the Backup Operators group.
 - D. **Incorrect:** Allow logon locally is a privilege for the Backup Operators group.
3. **Correct answer:** A
 - A. **Correct:** Site server is the core functionality for System Center.
 - B. **Incorrect:** Component server is not the core functionality for System Center.
 - C. **Incorrect:** Core server is not a valid functionality.
 - D. **Incorrect:** Site Core server is not a valid functionality.
4. **Correct answers:** B, C
 - A. **Incorrect:** All is a built-in scope.
 - B. **Correct:** System is not a built-in scope.
 - C. **Correct:** Administrator is not a built-in scope.
 - D. **Incorrect:** Default is a built-in scope.

Objective 1.2: Thought experiment

1. There are several performance indicators that can be examined, including the GC Response time, as well as GC Search Time and AD General Response.
2. Operations Manager contains the performance monitoring and alerts for this scenario.

Objective 1.2: Review

1. **Correct answer:** A
 - A. Correct:** AdtAdmin /setquery is the correct command to change the audit event filter.
 - B. Incorrect:** AdtAdmin /addFilter doesn't perform the requested action.
 - C. Incorrect:** AcsAdmin is not a valid command.
 - D. Incorrect:** AcsFilter /add is not a valid command.
2. **Correct answer:** C
 - A. Incorrect:** Operator does not have this privilege.
 - B. Incorrect:** Knowledge Administrator is not a valid role.
 - C. Correct:** Author has this privilege.
 - D. Incorrect:** Management Pack Administrator is not a valid role.
3. **Correct answer:** D
 - A. Incorrect:** NTDS should be monitored.
 - B. Incorrect:** NetLogon should be monitored.
 - C. Incorrect:** DFSR should be monitored.
 - D. Correct:** ADMon is not a valid service.
4. **Correct answer:** B
 - A. Incorrect:** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ADT\Parameters is not a valid path.
 - B. Correct:** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AdtServer\Parameters is the correct path.
 - C. Incorrect:** HKEY_LOCAL_MACHINE\User\CurrentWindowsServices\AdtServer\Parameters does not exist.
 - D. Incorrect:** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AdtSvc\Parameters is not a valid path.

Objective 1.3: Thought experiment

Update baselines are used to maintain updates on virtual machines. Update baselines are coordinated with a WSUS server, and an administrator chooses the appropriate updates for a given baseline. Sample baselines are included to provide a starting point.

DCM enables advanced configuration items to be tracked across a Configuration Manager deployment. For example, a registry setting can be monitored and changed (remediated) automatically using DCM.

Objective 1.3: Review

1. Correct answer: B

- A. Incorrect:** New-SCBaseline is not a valid command.
- B. Correct:** Create-SCBaseline is the correct command for this question.
- C. Incorrect:** SCBaseline /new is not a valid command.
- D. Incorrect:** New-VMMBaseline is not a valid command.

2. Correct answer: C

- A. Incorrect:** Configuration Item can be used as a setting for DCM.
- B. Incorrect:** Software Update can be used as a setting for DCM.
- C. Correct:** Configuration Agent is not a setting used with DCM.
- D. Incorrect:** Configuration Baseline can be used with DCM.

3. Correct answer: C

- A. Incorrect:** One day is not the default frequency.
- B. Incorrect:** One hour is not the default frequency.
- C. Correct:** 10 minutes is the default direct optimization frequency.
- D. Incorrect:** 24 hours is not the correct frequency.

This page intentionally left blank

Index

A

- access-based enumeration settings, 83–84
- access solutions
 - AD RMS, 242–255
 - client deployment, 245–246
 - federated identity support, 250–254
 - highly available deployment, 242–245
 - TPDs (trusted publishing domains), 249
 - TUDs (trusted user domains), 247–248
 - upgrading, migrating, and decommissioning, 254–255
- certificates
 - deployment, validation, and revocation, 221–223
 - key archival and recovery, 225–227
 - renewal, 223–224
 - templates, 217–221
- certificate services infrastructure, 189–215
 - administrator role separation, 209–211
 - CA migration, 209
 - Certificate Enrollment Policy Web Services, 201–204
 - Certificate Enrollment Web Services, 192–193, 201–204
 - configuring NDES, 204–205
 - configuring offline root CA, 196–201
 - disaster recovery, 194
 - monitoring CA health, 214–215
 - multi-forest CA deployment and trust, 192
 - multi-tier certification authority hierarchy, 190–191
 - NDES (Network Device Enrollment Services), 193
 - planning for validation and revocation, 193–194
 - trust between organizations, 211–214
- ACS (Audit Collection Services), 22–25
- ACS Collectors, 22
- ACS Database, 22
- ACS Forwarders, 22
- actions allowed, Tenant Administrator (VMM user role profile), 123
- Active/Active option, 96
- Active Directory. *See* AD (Active Directory)
- Active Directory database monitoring (AD monitoring scenario), 30
- Active Directory Federation Services. *See* AD FS
- Active Directory Rights Management Services. *See* AD RMS
- Active/Passive option, 96
- AD (Active Directory)
 - monitoring, 27
 - recovering domains and forests, 102–103
 - restoring objects and containers, 103–104
- Add/Edit Port Rule dialog box, 69–70
- /AddGroup parameter (AdtAdmin), 24
- Add IP Address dialog box, 66–67
- Add Load Balancer button, 73
- Add Operations Manager Wizard, 41–42
- Add Physical Disk dialog box, 78–79
- Add Relying Party Trust Wizard, 231
- Add Revocation Configuration Wizard, 206
- Add-SCCustomPlacementRule cmdlet, 140
- Add-SCStorageProvider cmdlet, 160, 163
- Add Storage Devices Wizard, 160–162
- Add Transform Claim Rule Wizard, 233
- Add-VMHardDiskDrive cmdlet, 136
- Add VM Network button, 73
- Add-WindowsFeature fs-iscsitarget-server command, 90

AD FS (Active Directory Federation Services)

- AD FS (Active Directory Federation Services), 228–240
 - attribute stores, 235–236
 - certificates, 237–238
 - claims-based authentication, 229–232
 - configuring claims rules, 232–235
 - identity integration with cloud services, 238–239
 - integrating with Web Application Proxy, 239–240
- AD FS Federation Server Configuration Wizard, 230
- AD FS Management tool, 237
- administration, delegating in VMM, 119–126
- administrative model, design
 - delegation, 11–18
 - Configuration Manager, 14
 - designing delegation, 14
 - Operations Manager, 16–18
 - role-based administration, 11–13
 - site system roles, 14–16
 - rights delegation for private cloud, 19–20
 - self-service portal design, 18
 - server infrastructure, 1–20
 - built-in groups, 6–11
 - delegation, 11–18
 - groups, 2
 - user rights, 3–6
- administrator role separation, certificate services
 - infrastructure, 209–211
- Administrators group, 7
- AD RMS (Active Directory Rights Management Services), 242–255
 - client deployment, 245–246
 - federated identity support, 250–254
 - highly available deployment, 242–245
 - TPDs (trusted publishing domains), 249
 - TUDs (trusted user domains), 247–248
 - upgrading, migrating, and decommissioning, 254–255
- AD RMS Certification Server Cluster, 242
- AD RMS Client, 242
- AD RMS Licensing-Only Cluster, 242
- AD RMS Service Group, 243
- AdtAdmin.exe command-line tool, 24
- AdtAdmin /getquery cmdlet, 24

- Advanced Quorum Configuration and Witness
 - Selection option (Configure Cluster Quorum Wizard), 61
- AIA (Authority Information Access) extension, 208
- alert connectors, Operations Manager, 177–178
- All Hosts group, viewing VM placement rules, 139
- Anonymous Logon Special Identity, 10
- App Controller, managing the private cloud, 19
- Application Administrator (VMM user role profile), 118
- Application Catalog web service point (site system role), 15
- Application Catalog website point (site system role), 15
- applications, high availability, 98
- archived rights policy templates, 252
- Asset Intelligence synchronization point (site system role), 15
- Assign Cloud, 20–21
- Assignment Scope page (Update Baseline Wizard), 35
- attribute stores, configuring, 235–236
- Audit Collection Services (ACS), 22–25
- Auditor role, certificate management, 210
- authentication, claims-based, 229–232
- authoritative restore, restoring objects and containers, 103–104
- Authority Information Access (AIA) extension, 208
- authorization rule templates, 234
- automated deployment, NLB, 72–74
- automated remediation, 32–47
 - configuring VMM to move a VM dynamically, 43–44
 - DCM baselines, 36–39
 - DSC solution, 45–47
 - update baselines, 33–36
 - VMM integration with Operations Manager, 39–43
- availability sets, highly available VMs, 132

B

- Background Intelligent Transfer Service (BITS), 166
- BackOffThreshold ACS setting, 23
- backup and recovery
 - server virtualization infrastructure, 180–181
 - strategy, 101
- Back up files and directories right, permissions, 3

- backup operator role, certificate management, 210
- Backup Operators group, 7
- bare metal, deploying Hyper-V hosts to, 130
- baselines
 - DCM (Desired Configuration Management)
 - baselines, 36–39
 - update baselines, 33–36
- BITS (Background Intelligent Transfer Service), 166
- block storage, 159
- bridge CAs, 192
- built-in certificate template properties, 219
- built-in container, groups, 8–9
- built-in groups, 6–11
- business continuity, 100–109
 - backup and recovery strategy, 101
 - Hyper-V Recovery Manager, 102
 - Hyper-V Replica, 102
 - recovering AD domains and forests, 102–103
 - restoring AD objects and containers, 103–104
 - System Center DPM, 104–110

C

- CA administrator role, certificate management, 210
- CA (certification authority)
 - configuring and managing offline root CA, 196–201
 - deployment and trust, 192
 - migration, 209
 - multi-tier hierarchy, 190–191
- CAU (Cluster Aware Updating), 62–63
- CAU plug-ins, 63
- CDP (CRL Distribution Point) extension, 200
- CEP (Certificate Enrollment Policy Web Services),
 - configuring, 201–204
- certificate-based authentication, DPM, 106
- Certificate Enrollment Policy Web Services (CEP),
 - configuring, 201–204
- Certificate Enrollment Web Services. *See* CES
- Certificate Enrollment Wizard, 221–222
- certificate manager role, certificate management, 210
- Certificate registration point (site system role), 15
- Certificate Revocation Lists (CRLs), 193
- certificates
 - deployment, validation, and revocation, 221–223
 - key archival and recovery, 225–227
 - planning for validation and revocation, 193–194
 - renewal, 223–224
 - service communications, 237
 - templates, 217–221
 - token decrypting, 237
 - token signing, 237
- certificate services infrastructure
 - design, 189–194
 - Certificate Enrollment Web Services, 192–193
 - disaster recovery, 194
 - multi-forest CA deployment and trust, 192
 - multi-tier certification authority
 - hierarchy, 190–191
 - NDES (Network Device Enrollment Services), 193
 - planning for validation and revocation, 193–194
 - implementation and management, 196–215
 - administrator role separation, 209–211
 - CA migration, 209
 - Certificate Enrollment Policy Web Services, 201–204
 - Certificate Enrollment Web Services, 201–204
 - configuring NDES, 204–205
 - configuring offline root CA, 196–201
 - monitoring CA health, 214–215
 - trust between organizations, 211–214
- Certificates MMC snap-in, 221
- Certificate Templates Console, 217–218
- Certificate Trust Lists (CTLs), 192
- Certificate Trust List Wizard, 213–214
- certification authority. *See* CA (certification authority)
- Cert Publishers group, 9
- CES (Certificate Enrollment Web Services)
 - configuring, 201–204
 - planning for, 192–193
- CI connectors, Operations Manager, 177–178
- Citrix XenServer, 129, 169
- claims-based authentication, 229–232
- claims provider trusts
 - claim rules, 232–235
 - claims-based authentication, 229–232
- claims rules, 232–235
- classes, 29

client deployment, AD RMS

- client deployment, AD RMS, 245–246
- cloud services, identity integration and, 238–239
- Cluster Aware Updating (CAU), 62–63
- clustered file servers, 97
- clustered storage, Hyper-V, 159–162
- Cluster Group Properties dialog box, 57–58
- clustering, 53–64
 - CAU (Cluster Aware Updating), 62–63
 - Heartbeat and DNS settings, 58
 - network redundancy and priority, 56–57
 - Quorum configuration, 59
 - resource failover and failback, 57–59
 - storage placement and replication, 62–63
- Cluster IP Addresses page (New Cluster Wizard), 68
- cluster parameters, configuring, 68
- Cluster Parameters tab (Properties dialog box), 71
- cluster-shared volumes (CSV), 53, 136
- cluster transfers, 165
- cmdlets. *See also* commands
 - Add-SCCustomPlacementRule, 140
 - Add-SCStorageProvider, 160, 163
 - Add-VMHardDiskDrive, 136
 - AdtAdmin /getquery, 24
 - Disable-NetAdapterRdma, 93
 - Get-Cluster, 55
 - Get-Cluster | Format-List, 58
 - Get-ClusterNode, 62
 - Get-ClusterParameter, 59
 - Get-ClusterQuorum, 62
 - Get-ClusterResource, 59
 - Get-MPIOSetting, 90
 - Get-MSDSMGlobalDefaultLoadBalancePolicy, 90
 - Get-Privilege, 6
 - Get-SCCustomPlacementRule, 140
 - Get-SCUserRole, 125
 - Get-SCUserRoleMembership, 125
 - Grant-Privilege, 6
 - Grant-SCResource, 125
 - Import-SCOMManagementPack, 27
 - New-SCBaseline, 36
 - New-SCOpsMgrConnection, 43
 - New-SCUserRole, 125
 - Remove-SCCustomPlacementRule, 140
 - Remove-SCUserRole, 125
 - Revoke-Privilege, 6
 - Revoke-SCResource, 125
 - Save-CauDebugTrace, 63
 - Set-ADFSProperties, 238
 - Set-NetOffloadGlobalSetting -NetworkDirect
 - Disabled, 93
 - Set-SCBaseline, 36
 - Set-SCCustomPlacementRule, 140
 - Set-SCUserRole, 125
 - Test-Privilege, 6
 - Test-SCPROTip, 177
- collections, role-based administration, 12
- collector queue settings (ACS), 23
- commands. *See also* cmdlets
 - Add-WindowsFeature fs-iscsitarget-server, 90
 - pkview, 214
 - Set-MPIOSetting, 90
 - wbadmin start systemstaterecovery, 102
- Compatibility tab, certificate templates, 220
- Component server (site system role), 15
- Configuration Manager, 14–16, 222
- Configure Applications page (Create VM Template Wizard), 142–143
- Configure Cluster Quorum Wizard, 60–61
- Configure Hardware page (Create VM Template Wizard), 140–141
- Configure Operating System page (Create VM Template Wizard), 142–143
- configuring
 - attribute stores, 235–236
 - Certificate Enrollment Policy Web Services, 201–204
 - Certificate Enrollment Web Services, 201–204
 - cluster parameters (NLB), 68
 - exclusion policies, 252–254
 - failover clustering storage, 62–63
 - Global Service Monitor, 26
 - Heartbeat and DNS settings, 58
 - IP address and MAC address settings, 150–156
 - iSCSI Target, 90–92
 - iSNS Server, 90–92
 - Library Servers (Create User Role Wizard), 122
 - live and storage migration between Hyper-V hosts
 - and clouds, 165–168
 - MPIO (multi-path I/O), 88–90

- multicast and unicast settings, 71–72
 - NDES (Network Device Enrollment Services), 204–205
 - network optimization, 156–157
 - network priority, 56–57
 - NLB (Network Load Balancing), 65–69
 - offline root CA, 196–201
 - Quorum, 59–61
 - replication group schedule, 87
 - resource failover and failback, 57–59
 - Run As Accounts (Create User Role Wizard), 122
 - storage pools, 77–79
 - VMM (Virtual Machine Manager)
 - logical networks, 146–150
 - storage devices, 161
 - dynamic movement, 43–44
 - user role memberships, 121
 - placement rules, 136–140
 - Connection Details page (Operations Manager Settings dialog box), 176
 - Connection To Operations Manager page (Add Operations Manager Wizard), 42
 - connectors, Operations Manager, 177–178
 - Connect To Server dialog box, 123–124
 - constant names, security-related user rights, 3–6
 - continuously available file shares, 97
 - converged networks, 150
 - Convert Physical Server (P2V) Wizard, 169–170
 - CPU percentage parameter (host reserves), 127
 - CPU resource threshold, dynamic optimization, 173
 - Create Configuration Baseline dialog box, 36–37
 - Create Custom Requirement dialog box, 139
 - Create Logical Network Wizard, 148–150
 - Create MAC Address Pool Wizard, 153–154
 - Create New Protection Group Wizard, 106
 - Create Static IP Address Pool Wizard, 151–153
 - Create User Role Wizard, 17, 119–124
 - Create VM Network Wizard, 154–156
 - Create VM Template Wizard, 140–144
 - creating
 - equivalent objects, 126–127
 - storage pools, 77–79
 - Storage Spaces, 79–82
 - VMM logical networks, 148–150
 - VMM templates, 140–144
 - VMM user roles, 120
 - VM networks, 154–156
 - CRL Distribution Point (CDP) extension, 200
 - CRLs (Certificate Revocation Lists), 193
 - cross-certification CAs, 192
 - CrossSubnetDelay parameter
 - (Get-Cluster | Format-List cmdlet), 58
 - CrossSubnetThreshold parameter
 - (Get-Cluster | Format-List cmdlet), 58
 - Cryptographic Operators group, 7
 - cryptographic service providers (CSPs), 205
 - Cryptography tab, certificate templates, 220
 - CSPs (cryptographic service providers), 205
 - CSV (cluster-shared volumes), 53, 136
 - CSV storage, 160–162
 - CTLs (Certificate Trust Lists), 192
- ## D
- DatabaseReadWriteMode property
 - (Get-Cluster cmdlet), 55
 - Data Center Management Interface (DCMI), 130
 - Data Protection Manager (DPM), 104–110, 180–181
 - DCM (Desired ConfigurationManagement)
 - baselines, 36–39
 - DCMI (Data Center Management Interface), 130
 - decommission.asmx URL, 255
 - decommissioning AD RMS, 254–255
 - default groups, 6–11
 - delegation
 - administrative model design, 11–18
 - Configuration Manager, 14
 - designing delegation, 14
 - Operations Manager, 16–18
 - role-based administration, 11–13
 - site system roles, 14–16
 - virtual environment, 118–125
 - self-service in VMM, 125
 - VMM, 118–125
 - Deleted Objects container (Active Directory Recycle Bin), 103
 - /DelGroup parameter (AdtAdmin), 24

deny rule, claims

- deny rule, claims, 235
- Deploy Configuration Baselines dialog box, 37–38
- deployment
 - AD RMS (Active Directory Rights Management Services), 242–246
 - certificates, 221–223
 - Hyper-V hosts to bare metal, 130
 - multi-forest CA, 192
- design
 - administrative model, 1–20
 - built-in groups, 6–11
 - delegation, 11–18
 - groups, 2
 - rights delegation for private clouds, 19–20
 - self-service portal design, 18
 - user rights, 3–6
 - AD RMS, 242–255
 - client deployment, 245–246
 - federated identity support, 250–254
 - highly available deployment, 242–245
 - trusted publishing domains, 249
 - TUDs (trusted user domains), 247–248
 - upgrading, migrating, and decommissioning, 254–255
 - certificate services infrastructure, 189–194
 - Certificate Enrollment Web Services, 192–193
 - disaster recovery, 194
 - multi-forest CA deployment and trust, 192
 - multi-tier certification authority hierarchy, 190–191
 - NDES (Network Device Enrollment Services), 193
 - planning for validation and revocation, 193–194
 - federated identity solutions, 228–240
 - AD FS certificates, 237–238
 - claims-based authentication, 229–232
 - claims provider and relying-party trust claim rules, 232–235
 - configuring attribute stores, 235–236
 - identity integration with cloud services, 238–239
 - integrating Web Application Proxy with AD FS, 239–240
 - highly available failover clustering, 56–57
 - highly available network services, 70–71
 - monitoring strategy
 - ACS (Audit Collection Services), 22–25
 - Active Directory monitoring, 27
 - Global Service Monitor, 25–26
 - management packs, 27–29
 - Desired Configuration Management (DCM) baselines, 36–39
 - Desired State Configuration (DSC), 45–47
 - device-specific modules (DSMs), 88
 - DFS Namespaces (DFSN or DFS-N), 82–88
 - DFS-N (DFS Namespaces), 82–88
 - DFSN (DFS Namespaces), 82–88
 - DFS-R (DFS Replication), 82–88
 - DFSR (DFS Replication), 82–88
 - DFS Replication (DFSR or DFS-R), 82–88
 - DHCP (Dynamic Host Configuration Protocol), high availability, 95–96
 - DHCP Manager tool, 95
 - dialog boxes
 - Add/Edit Port Rule, 69–70
 - Add IP Address, 66–67
 - Add Physical Disk, 78–79
 - Cluster Group Properties, 57–58
 - Connect To Server, 123–124
 - Create Configuration Baseline, 36–37
 - Create Custom Requirement, 139
 - Deploy Configuration Baselines, 37–38
 - Dynamic Optimization, 44
 - Edit Rule, 38–39
 - Edit Settings, 84–85
 - Equivalent Library Objects, 126–127
 - Exclude User, 252–253
 - Import Trusted Publishing Domain, 249
 - Import Trusted User Domain, 247
 - Live Migration Settings, 57
 - Lockbox Version, 254
 - Manage Custom Properties, 138
 - MPIO Properties, 89
 - Operations Manager Settings, 175–176
 - Revocation Provider Properties, 207
 - Select User Role, 123–124
 - Settings, 174
 - Virtual Switches, 150
 - Directory service availability (AD monitoring scenario), 30

- directory synchronization, 238
- Directory Synchronization tool, 239
- Disable-NetAdapterRdma cmdlet, 93
- Disable This Port Range filtering mode, NLB clusters, 71
- disaster recovery, 100–109
 - backup and recovery strategy, 101
 - certificate services infrastructure, 194
 - Hyper-V Recovery Manager, 102
 - Hyper-V Replica, 102
 - recovering AD domains and forests, 102–103
 - restoring AD objects and containers, 103–104
 - System Center DPM, 104–110
- /Disconnect parameter (AdtAdmin), 24
- DisconnectThreshold ACS setting, 23
- disk I/O resource threshold, dynamic optimization, 174
- disk space parameter (host reserves), 128
- disk witness types, 60
- Distributed COM Users group, 7
- Distributed Network Name feature, 97
- Distribution point (site system role), 15
- DnsAdmins group, 9
- DNS settings, configuring, 58
- DnsUpdateProxy group, 9
- Domain Admins group, 9
- Domain Computers group, 10
- Domain Controllers group, 10
- Domain Guests group, 10
- Domain Local group scope, 2
- domains, recovering, 102–103
- Domain Users group, 10
- DPM agents, installation, 104
- DPM (Data Protection Manager), 104–110, 180–181
 - implementing deployment, 106–110
 - planning deployment, 105–106
- DSC (Desired State Configuration), 45–47
- DSMs (device-specific modules), 88
- DSM settings, 88
- Dynamic Host Configuration Protocol (DHCP), high
 - availability, 95–96
- dynamic memory, guest resource optimization, 134
- dynamic optimization
 - configuring VMM to move VMs, 43–44
 - server virtualization infrastructure, 172–175
- Dynamic Optimization dialog box, 44

E

- Edit Rule dialog box, 38–39
- Edit Settings dialog box, 84–85
- enabling ACS forwarders, 23
- Endpoint Protection point (site system role), 15
- enrollee role, certificate management, 210
- Enrollment point proxy (site system role), 15
- Enrollment point (site system role), 15
- Enterprise Admins group, 10
- enterprise root CAs, 190
- Equivalent Library Objects dialog box, 126–127
- equivalent objects, 126–127
- Essential services (AD monitoring scenario), 30
- ESX hosts, 129
- Everyone Special Identity, 10
- Exclude User dialog box, 252–253
- exclusion policies, configuring, 252–254
- Expected Utilization, configuring VM placement, 137
- Extensions tab, certificate templates, 220
- external root CAs, 190
- external virtual switches, 151

F

- Fabric Administrator (VMM user role profile), 118
- Fabric workspace, 129
- failback, configuring, 57–59
- failover clustering, 53–64
 - CAU (Cluster Aware Updating), 62–63
 - design considerations, network redundancy and priority, 56–57
 - Heartbeat and DNS settings, 58
 - planning and implementation, 54–56
 - Quorum configuration, 59–61
 - resource failover and failback, 57–59
 - storage placement and replication, 62–63
- Failover Cluster Manager, 53, 136
- Failover Cluster Validation Report, 54
- Failover Only DSM setting, 88
- Fallback status point (site system role), 16
- fault-tolerant networking, 70–71
- federated identity solutions, 228–240

Federation Service, AD FS

- AD FS certificates, 237–238
 - claims-based authentication, 229–232
 - claims provider and relying-party trust claim rules, 232–235
 - configuring attribute stores, 235–236
 - identity integration with cloud services, 238–239
 - integrating Web Application Proxy with AD FS, 239–240
 - support for AD RMS, 250–254
- Federation Service, AD FS, 229
- Fibre Channel, 162–163
- file locations, AD RMS client, 245
- file shares
- high availability, 97
 - witness types, 60
- file storage, 159
- fixed provisioning, 80
- forests, recovering, 102–103
- full mesh topology, 86

G

- gateways, VM networks, 156
- General tab, certificate templates, 220
- Generic Application option, 98
- generic failover clustering, 98
- Generic Script option, 98
- Generic Service option, 98
- Get-Cluster cmdlet, 55
- Get-Cluster | Format-List cmdlet, 58
- Get-ClusterNode cmdlet, 62
- Get-ClusterParameter cmdlet, 59
- Get-ClusterQuorum cmdlet, 62
- Get-ClusterResource cmdlet, 59
- /GetDBAuth parameter (AdtAdmin), 24
- Get-MPIOSetting cmdlet, 90
- Get-MSDSMGlobalDefaultLoadBalancePolicy cmdlet, 90
- Get-Privilege cmdlet, 6
- /GetQuery parameter (AdtAdmin), 24
- Get-SCCustomPlacementRule cmdlet, 140
- Get-SCUserRole cmdlet, 125
- Get-SCUserRoleMembership cmdlet, 125
- Global group scope, 2
- Global Service Monitor, 25–26
- Grant-Privilege cmdlet, 6
- Grant-SCResource cmdlet, 125
- Group Policy, deploying certificates, 222
- Group Policy Creator Owners group, 10
- groups, 2
- built-in container, 8–9
 - special identities, 10–11
 - Users container, 9–10
- Guest OS Profile option, configuring operating system settings for VM template, 142
- guest resource optimization, VMs, 134–136
- Guests group, 7
- guest storage, Hyper-V, 162–163
- GUM, communicating cluster updates, 55

H

- Heartbeat settings, configuring, 58
- high availability
- business continuity and disaster recovery, 100–109
 - backup and recovery strategy, 101
 - Hyper-V Recovery Manager, 102
 - Hyper-V Replica, 102
 - recovering AD domains and forests, 102–103
 - restoring AD objects and containers, 103–104
 - System Center DPM, 104–110
- failover clustering, 53–64
- CAU (Cluster Aware Updating), 62–63
 - Heartbeat and DNS settings, 58
 - network redundancy and priority, 56–57
 - planning and implementation, 54–56
 - Quorum configuration, 59–61
 - resource failover and fallback, 57–59
 - storage placement and replication, 62–63
- network services, 65–74
- automated deployment of NLB using VMM templates, 72–74
 - fault-tolerant networking, 70–71
 - multicast vs unicast configuration, 71–72
 - NLB (Network Load Balancing), 65–69
 - state management, 72

- server roles, 95–99
 - applications, services, and scripts, 98
 - continuously available file shares, 97
 - DHCP, 95–96
 - Hyper-V clustering, 96–97
 - storage solutions, 76–93
 - iSCSI Target and ISNS Server, 90–92
 - MPIO (multi-path I/O), 88–90
 - multi-replica DFS Namespaces, 82–88
 - RDMA (Remote Directory Memory Access), 92–93
 - SMB multichannel, 92–93
 - Storage Spaces and storage pools, 76–82
 - High Availability Wizard, 91
 - highly available VMs, server virtualization, 132–133
 - Host Parameters page (New Cluster Wizard), 66–67
 - HostRecordTTL property, 59
 - host reserves, 127
 - hosts, server virtualization, 117–130
 - deploying Hyper-V hosts to bare metal, 130
 - multi-host libraries, 125–127
 - resource optimization, 127–128
 - third-party virtualization platforms, 129–130
 - virtual environment delegation, 118–125
 - hub and spoke topology, 86
 - Hyper-V
 - clustered storage, 159–162
 - clustering, 96–97
 - configuring IP and MAC address settings across hosts, 150–156
 - configuring live and storage migration between hosts and clouds, 165–168
 - deploying hosts to bare metal, 130
 - guest storage, 162–163
 - live migrations, 57
 - Hyper-V Recovery Manager, 102
 - Hyper-V Replica, 102
 - Hyper-V Replica Broker cluster service, 102
- I**
- identity integration with cloud services, 238–239
 - identity solutions
 - AD RMS, 242–255
 - client deployment, 245–246
 - federated identity support, 250–254
 - highly available deployment, 242–245
 - trusted publishing domains, 249
 - TUDs (trusted user domains), 247–248
 - upgrading, migrating, and decommissioning, 254–255
 - certificates
 - deployment, validation, and revocation, 221–223
 - key archival and recovery, 225–227
 - renewal, 223–224
 - templates, 217–221
 - certificate services infrastructure, 189–194, 196–215
 - administrator role separation, 209–211
 - CA migration, 209
 - Certificate Enrollment Policy Web Services, 201–204
 - Certificate Enrollment Web Services, 192–193, 201–204
 - configuring NDES, 204–205
 - configuring offline root CA, 196–201
 - disaster recovery, 194
 - monitoring CA health, 214–215
 - multi-forest CA deployment and trust, 192
 - multi-tier certification authority hierarchy, 190–191
 - NDES (Network Device Enrollment Services), 193
 - planning for validation and revocation, 193–194
 - trust between organizations, 211–214
 - federated identity solutions, 228–240
 - AD FS certificates, 237–238
 - claims-based authentication, 229–232
 - claims provider and relying-party trust claim rules, 232–235
 - configuring attribute stores, 235–236
 - identity integration with cloud services, 238–239
 - integrating Web Application Proxy with AD FS, 239–240
 - IIS_IUSRS group, 7
 - IIS_WPG group, 10
 - implementation
 - AD RMS, 242–255
 - client deployment, 245–246

Import Management Packs tool

- federated identity support, 250–254
- highly available deployment, 242–245
- trusted publishing domains, 249
- TUDs (trusted user domains), 247–248
- upgrading, migrating, and decommissioning, 254–255
- automated remediation, 32–47
 - configuring VMM to move a VM dynamically, 43–44
 - DCM baselines, 36–39
 - DSC solution, 45–47
 - update baselines, 33–36
 - VMM integration with Operations Manager, 39–43
- certificates
 - deployment, validation, and revocation, 221–223
 - key archival and recovery, 225–227
 - renewal, 223–224
 - templates, 217–221
- certificate services infrastructure, 196–215
 - administrator role separation, 209–211
 - CA migration, 209
 - Certificate Enrollment Policy Web Services, 201–204
 - Certificate Enrollment Web Services, 201–204
 - configuring NDES, 204–205
 - configuring offline root CA, 196–201
 - monitoring CA health, 214–215
 - trust management, 211–214
- DPM deployment, 106–110
- federated identity solutions, 228–240
 - AD FS certificates, 237–238
 - claims-based authentication, 229–232
 - claims provider and relying-party trust claim rules, 232–235
 - configuring attribute stores, 235–236
 - identity integration with cloud services, 238–239
 - integrating Web Application Proxy with AD FS, 239–240
- high availability
 - business continuity and disaster recovery, 100–109
 - failover clustering, 53–64
 - network services, 65–74
- server roles, 95–99
- storage solutions, 76–93
- management packs, 27–28
- server virtualization
 - hosts, 117–130
 - managing and maintaining infrastructure, 172–181
 - networking, 146–158
 - storage, 159–163
 - VM movement, 165–170
 - VMs (virtual machines), 132–144
- Import Management Packs tool, 28
- Import Management Packs Wizard, 27
- Import-SCOMManagementPack cmdlet, 27
- Import Trusted Publishing Domain dialog box, 249
- Import Trusted User Domain dialog box, 247
- Incoming Forest Trust Builders group, 9
- infrastructure
 - certificate services. *See* certificate services infrastructure
 - high availability
 - business continuity and disaster recovery, 100–109
 - failover clustering, 53–64
 - network services, 65–74
 - server roles, 95–99
 - storage solutions, 76–93
 - servers
 - administrative model, 1–20
 - automated remediation, 32–47
 - monitoring strategy, 22–30
 - server virtualization
 - hosts, 117–130
 - managing and maintaining infrastructure, 172–181
 - networking, 146–158
 - storage, 159–163
 - VM movement, 165–170
 - VMs (virtual machines), 132–144
- installation
 - Certification Authority role service, 197
 - DPM agents, 104
 - Operations Manager agent, 40
- Integrated Scripting Environment (ISE), 45

- Intelligent Platform Management Interface (IPMI), 130
- Interactive mode, installing AD RMS client, 245
- Interactive Special Identity, 10
- intermediate tier (CA hierarchy), 191
- internal virtual switches, 151
- Internet Server API (ISAPI), 193
- Internet Small Computer System Interface (iSCSI), 90
- Internet Storage Name Service (iSNS), 90
- IP addresses, configuring settings across Hyper-V hosts, 150–156
- IP address pools
 - configuring, 151–153
 - VMM logical networks, 147
- IPMI (Intelligent Platform Management Interface), 130
- ISAPI (Internet Server API), 193
- iSCSI (Internet Small Computer System Interface), 90
- iSCSI Target, configuring, 90–92
- iSCSI Target Server, 163
- isDeleted attribute, 104
- ISE (Integrated Scripting Environment), 45
- iSNS (Internet Storage Name Service), 90
- iSNS Server, configuring, 90–92
- isolation type, VM networks, 155
- Issuance Requirements tab, certificate templates, 220
- issuing tier (CA hierarchy), 190

K

- key archival, certificates, 225–227
- Key Recovery Agent template, 225–226
- knowledge, optimizing management packs, 29

L

- Least Blocks DSM setting, 88
- Least Queue Depth DSM setting, 88
- Library Servers (Create User Role Wizard), 122
- license locations, AD RMS client, 245
- lifecycle, management packs, 27
- /ListForwarders parameter (AdtAdmin), 24
- /ListGroup parameter (AdtAdmin), 24
- live migrations, configuring between Hyper-V hosts and clouds, 165–168

- Live Migration Settings dialog box, 57
- Load Balancer, 73
- local groups, user rights, 7–11
- Lockbox Version dialog box, 254
- logical networks (VMM), configuring, 146–150

M

- MAC addresses, configuring settings across Hyper-V hosts, 150–156
- MAC address pools
 - configuring, 153–154
 - VMM logical networks, 148
- maintenance
 - server infrastructure
 - administrative model, 1–20
 - automated remediation, 32–47
 - monitoring strategy, 22–30
 - server virtualization infrastructure, 172–181
 - backup and recovery using DPM, 180–181
 - dynamic and resource optimization, 172–175
 - integration of Operations Manager with VMM and Service Manager, 175–179
 - updating VM images in libraries, 179–180
- Manage Custom Properties dialog box, 138
- management
 - certificates
 - deployment, validation, and revocation, 221–223
 - key archival and recovery, 225–227
 - renewal, 223–224
 - templates, 217–221
 - certificate services infrastructure, 196–215
 - administrator role separation, 209–211
 - CA migration, 209
 - Certificate Enrollment Policy Web Services, 201–204
 - Certificate Enrollment Web Services, 201–204
 - configuring NDES, 204–205
 - configuring offline root CA, 196–201
 - monitoring CA health, 214–215
 - trust between organizations, 211–214
 - server infrastructure
 - administrative model, 1–20

- automated remediation, 32–47
- monitoring strategy, 22–30
- server virtualization infrastructure, 172–181
 - backup and recovery using DPM, 180–181
 - dynamic and resource optimization, 172–175
 - integration of Operations Manager with VMM and Service Manager, 175–179
 - updating VM images in libraries, 179–180
- TPDs (trusted publishing domains), 249
- TUDs (trusted user domains), 247–248
- management packs, Operations Manager, 27–29
- Management point (site system role), 16
- manual migrations, 166
- maximum disk I/O per second parameter (host reserves), 128
- Maximum Memory dynamic memory setting, 134
- MaximumQueueLength ACS setting, 23
- membership, VMM Administrator user role, 119
- Memory Buffer Percentage dynamic memory setting, 134
- memory parameter (host reserves), 127
- memory resource threshold, dynamic optimization, 173
- Memory Weight setting, 135
- Microsoft accounts, AD RMS, 243
- Microsoft Azure, Hyper-V Recovery Manager, 102
- Microsoft Operations Framework (MOF) files, 46
- Migrate VM Wizard, 166
- migrating
 - AD RMS (Active Directory Rights Management Services), 254–255
 - CA (certification authority), 209
- Minimum Memory dynamic memory setting, 134
- mirror resiliency, 77
- MOF (Microsoft Operations Framework) files, 46
- monitoring CA health, 214–215
- monitoring strategy, design, 22–30
 - ACS (Audit Collection Services), 22–25
 - Active Directory monitoring, 27
 - Global Service Monitor, 25–26
 - management packs, 27–29
- movement, VMs (virtual machines), 165–170
 - live and storage migration between Hyper-V hosts and clouds, 165–168
 - P2V and V2V, 168–170

- MPIO (multi-path I/O), 88–90
- MPIO Properties dialog box, 89
- msDS-deletedObjectLifetime attribute, 103
- multicast settings, configuring NLB, 71–72
- multi-forest CA deployment, 192
- multi-forest monitoring (AD scenario), 30
- multi-host libraries, server virtualization, 125–127
- multi-path I/O (MPIO), 88–90
- Multiple Hosts filtering mode, NLB clusters, 71
- multi-replica DFS Namespaces, 82–88
- multi-tier certification authority hierarchy, 190–191

N

- NDES (Network Device Enrollment Services), 193, 204–205, 224
- network-based storage migrations, 166–167
- network capacity percentage parameter (host reserves), 128
- Network Configuration Operators group, 7, 9
- Network Device Enrollment Services (NDES), 193, 204–205, 224
- networking, server virtualization, 146–158
 - configuring IP address and MAC address settings, 150–156
 - configuring network optimization, 156–157
 - configuring VMM logical networks, 146–150
 - Windows Server Gateway, 157
- network I/O resource threshold, dynamic optimization, 174
- Network Load Balancing Manager, 65
- Network Load Balancing (NLB), 65–69, 72–74
- network redundancy, 56–57
- network services, high availability, 65–74
 - automated deployment of NLB using VMM templates, 72–74
 - fault-tolerant networking, 70–71
 - multicast vs unicast configuration, 71–72
 - NLB (Network Load Balancing), 65–69
 - state management, 72
- network sites, VMM logical networks, 147
- Network Special Identity, 10
- New Cluster Wizard, 66

- New-SCBaseline cmdlet, 36
- New-SCOpsMgrConnection cmdlet, 43
- New-SCUserRole cmdlet, 125
- New Storage Pool Wizard, 77
- New Trust Wizard, 211–212
- New Virtual Disk Wizard, 79
- New Volume Wizard, 82–83
- NLB (Network Load Balancing), 65–69, 72–74
- node majority types, Quorum configuration, 61
- node majority with witness types, Quorum configuration, 61
- no majority (disk witness only) type, Quorum configuration, 61
- No topology option, 86

O

- offline mode, P2V migrations, 168–169
- offline root CA, configuring, 196–201
- online mode, P2V migrations, 168
- Online Responder Manager, 206
- Online Responder service, 205
- Operations Manager, 16–18
 - integration with VMM, 39–43
 - integration with Service Manager, 175–179
 - monitoring strategy, 22–30
 - ACS (Audit Collection Services), 22–25
 - Global Service Monitor, 25–26
 - management packs, 27–29
 - profiles, 16
- Operations Manager Settings dialog box, 175–176
- Operations Manager Setup Wizard, 40
- Operations Master monitoring (AD monitoring scenario), 30
- optimization
 - configuring network optimization, 156–157
 - dynamic and resource optimization, 172–175
 - host resources, 127–128
 - management packs, 28–29
 - power optimization, 128
 - VM guest resources, 134–137
 - VMM storage, 163
- Optimize For Consistency option, 84
- Optimize For Scalability option, 84
- ordering method options, configuring referral settings, 85
- Out of band service point (site system role), 16
- Override Host Reserve Settings From The Parent Host Group check box, 128
- overrides, customizing management packs, 29

P

- P2V (physical to virtual) migrations, 168–170
- parameters
 - AdtAdmin, 24
 - DSC scripts, 46
- parity resiliency, 77
- partitioned clusters, 62
- pass-through disks, 163
- Performance and Resource Optimization (PRO) tips, 163, 175–178
- Performance Log Users group, 7, 9
- Performance Monitor Users group, 7, 9
- permissions
 - Back up files and directories right, 3
 - certificate management, 210–211
 - defined, 3
- permitted actions, Tenant Administrator (VMM user role profile), 123
- physical to virtual (P2V) migrations, 168–170
- pkview command, 214
- placement rules, virtual machines, 136–140
- planning
 - automated remediation, 32–47
 - configuring VMM to move a VM dynamically, 43–44
 - DCM baselines, 36–39
 - DSC solution, 45–47
 - update baselines, 33–36
 - VMM integration with Operations Manager, 39–43
- DPM deployment, 105–106
- high availability
 - business continuity and disaster recovery, 100–109

Plug and Play (PnP) Manager

- failover clustering, 53–64
- network services, 65–74
- server roles, 95–99
- storage solutions, 76–93
- server virtualization
 - hosts, 117–130
 - managing and maintaining
 - infrastructure, 172–181
 - networking, 146–158
 - storage, 159–163
 - VM movement, 165–170
 - VMs (virtual machines), 132–144
- Plug and Play (PnP) Manager, 88
- PnP (Plug and Play) Manager, 88
- polling settings, 83–84
- Port Rules page (New Cluster Wizard), 69
- ports, AD RMS requirements, 243
- power optimization, 128, 172–175
- Power Optimization Settings page (VMM), 174
- Power Users group, 7
- preferred VMM hosts, 132
- Pre-Windows 2000 Compatible Access group, 9
- Print Operators group, 9
- priority, 56–57, 133
- private cloud, rights delegation, 19–20
- private virtual switches, 151
- profiles, Operations Manager, 16
- PRO Monitor Configuration page (Operations Manager Settings dialog box), 177
- PRO (Performance and Resource Optimization)
 - tips, 163, 175–178
- properties, certificate templates, 218–219
- Protection Agent Installation Wizard, 104
- protection groups, 105
 - choosing replica method, 109
 - configuring protection schedule, 108
 - consistency check options, 110
 - data selection, 107
 - disk allocation, 109
 - setting parameters, 108
- protocols, AD RMS requirements, 243
- publishing intervals, CRLs, 194
- Publish New Application Wizard, 239

Q

- quick migrations, 165
- quick storage migrations, 165
- Quorum configuration, 59–61
- quotas, Tenant Administrator (VMM user role profile), 123

R

- RA (registration authority), 204
- RAS and IAS Servers group, 10
- RDC (Remote Differential Compression), 82
- RDMA (Remote Directory Memory Access), 92–93
- Read-Only Administrator (VMM user role profile), 118
- recovery
 - AD domains and forests, 102–103
 - certificates, 225–227
 - server virtualization infrastructure, 180–181
- Recycle Bin, restoring objects and containers, 103–104
- redundancy
 - clustered services, 56–57
 - Hyper-V clustering, 96–97
- referral settings, 85–86
- registration authority (RA), 204
- registry keys, AD RMS client, 246
- relying-party trusts
 - claim rules, 232–235
 - configuration options, 231–232
- Remote Desktop Users group, 7, 9
- Remote Differential Compression (RDC), 82
- Remote Directory Memory Access (RDMA), 92–93
- RemoteFX, 135
- remote-updating mode, CAU, 63
- Remove-SCCustomPlacementRule cmdlet, 140
- Remove-SCUserRole cmdlet, 125
- renewal, certificates, 221–224
- replication, failover clustering, 62–63
- Replication (AD monitoring scenario), 30
- replication group schedule, configuring, 87
- Replicators group, 7, 9
- Reporting services point (site system role), 16
- request-handling mode (CAs), 200

- Request Handling tab, certificate templates, 220
- resource failover, configuring, 57–59
- resource optimization, server virtualization
 - infrastructure, 172–175
- restoring AD objects and containers, 103–104
- revocation
 - certificates, 193–194, 221–223
 - configuration, online responders, 206
- Revocation Provider Properties dialog box, 207
- Revoke-Privilege cmdlet, 6
- Revoke-SCResource cmdlet, 125
- rights
 - delegation, private cloud, 19–20
 - policy templates, 250–252
 - user rights, 3–6
- role-based administration, 11–13
 - collections, 12
 - security roles, 12
 - security scopes, 13–14
- Role Of Partner Server as Standby mode, 96
- roles, administering a certificate infrastructure, 209–211
- root CA types, 190
- root tier (CA hierarchy), 190–191
- Round Robin DSM setting, 88
- Round Robin with Subset DSM setting, 88
- Run As Accounts (Create User Role Wizard), 122

S

- SameSubnetDelay parameter (Get-Cluster | Format-List cmdlet), 58
- SameSubnetThreshold parameter (Get-Cluster | Format-List cmdlet), 58
- SAN-based migrations, 167
- SAS (Serial Attached SCSI) disks, 77
- SATA (Serial Advanced Technology Attachment)
 - disks, 77
- Save-CauDebugTrace PowerShell cmdlet, 63
- scale-out file servers, 97, 136
- SCEP (Simple Certificate Enrollment Protocol), 193
- Schema Admins group, 10
- scope
 - authentication, New Trust Wizard, 212
 - groups, 2
 - VMM user roles, 121
- SCP (Service Connection Point), 244
- scripts, high availability, 98
- SCSI Primary Commands-3 (SPC-3) compliant
 - storage, 88
- security groups, 2
- security-related user rights, 3–6
- security roles, role-based administration, 12
- security scopes, role-based administration, 13–14
- Security tab, certificate templates, 220
- Select User Role dialog box, 123–124
- self-service
 - portal design, 18
 - VMM (Virtual Machine Manager), 125
- self-updating mode, CAU, 63
- Serial Advanced Technology Attachment (SATA)
 - disks, 77
- Serial Attached SCSI (SAS) disks, 77
- Server Operators group, 9
- server roles, high availability, 95–99
 - applications, services, and scripts, 98
 - continuously available file shares, 97
 - DHCP, 95–96
 - Hyper-V clustering, 96–97
- servers
 - infrastructure management
 - administrative model, 1–20
 - automated remediation, 32–47
 - monitoring strategy, 22–30
 - virtualization
 - hosts, 117–130
 - managing and maintaining
 - infrastructure, 172–181
 - networking, 146–158
 - storage, 159–163
 - VM movement, 165–170
 - VMs (virtual machines), 132–144
- Server tab, certificate templates, 220
- service communications certificates, 237
- Service Connection Point (SCP), 244
- Service Manager
 - integration with Operations Manager, 175–179
 - self-service portal design, 18

Service Template Designer

- Service Template Designer, 73
- Set-ADFSProperties cmdlet, 238
- /SetDBAuth parameter (AdtAdmin), 24
- Set-MPIOSetting command, 90
- Set-NetOffloadGlobalSetting -NetworkDirect Disabled cmdlet, 93
- /SetQuery parameter (AdtAdmin), 24
- Set-SCBaseline cmdlet, 36
- Set-SCCustomPlacementRule cmdlet, 140
- Set-SCUserRole cmdlet, 125
- settings
 - certificate templates, 220
 - collector queue (ACS), 23
 - DFS Namespaces, 83–86
 - DFS Replication, 86–88
 - DSMs (device-specific modules), 88
- Settings dialog box, 174
- Shared VHDx, 136–137
- Silent mode, installing AD RMS client, 245
- Simple Certificate Enrollment Protocol (SCEP), 193
- simple resiliency, 77
- Single Host filtering mode, NLB clusters, 71
- Site database server (site system role), 15
- Site server (site system role), 15
- site system roles, administrative model design, 14–16
- Site system (site system role), 15
- Smart Paging, 135
- SMASH (System Management Architecture for Server Hardware), 130
- SMB multichannel, implementing storage, 92–93
- SMB storage, 160–162
- SMS Provider (site system role), 15
- snapshots, 166
- Software update point (site system role), 16
- SPC-3 (SCSI Primary Commands-3) compliant storage, 88
- special identities, 10–11
- split brain clusters, 62
- split scope DHCP, 96
- SQL Servers
 - AD RMS, 242
 - configuring as part of VM template, 143
- standalone root CAs, 190, 197
- Startup Memory dynamic memory setting, 134
- state management, 72
- State migration point (site system role), 16
- static IP address pools, VMM logical networks, 147–148
- /Stats parameter (AdtAdmin), 24
- status, certificates, 223
- storage solutions
 - failover clustering, 62–63
 - high availability, 76–93
 - iSCSI Target and ISNS Server, 90–92
 - MPIO (multi-path I/O), 88–90
 - multi-replica DFS Namespaces, 82–88
 - RDMA (Remote Directory Memory Access), 92–93
 - SMB multichannel, 92–93
 - Storage Spaces and storage pools, 76–82
 - migration, configuring between Hyper-V hosts and clouds, 165–168
 - storage pools, 76–82
 - server virtualization, 159–163
 - Hyper-V clustered storage, 159–162
 - Hyper-V guest storage, 162–163
 - optimization, 163
- Storage Spaces, 76–82
- Subject Name tab, certificate templates, 220
- subnets, VM networks, 155
- subordinate CAs, 191
- Summary page (Add Operations Manager Wizard), 43
- Superseded Templates tab, certificate templates, 220
- System Health Validator point (site system role), 16
- System Management Architecture for Server Hardware (SMASH), 130

T

- targets, 29
- TCP Chimney Offload, 156
- templates
 - archived rights policy, 252
 - authorization rules, 234
 - certificates, 217–221
 - claims rules, 233
 - OCSP, 206
 - rights policy, 250–252

- VMM (Virtual Machine Manager), 140–144
- Tenant Administrator (VMM user role profile), 118, 123
- Test-Privilege cmdlet, 6
- Test-SCPROTip cmdlet, 177
- thin provisioning, 80
- third-party virtualization platforms, 129–130
- Time skew monitoring (AD monitoring scenario), 30
- token decrypting certificates, 237
- token signing certificates, 237
- tombstoneLifetime attribute, 103
- TPDs (trusted publishing domains), 243, 249
- trusted publishing domains (TPDs), 243, 249
- trusted user domains (TUDs), 242, 247–248
- trust management, certificate services, 192, 211–214
- Trust monitoring (AD monitoring scenario), 30
- TUDs (trusted user domains), 242, 247–248
- two-way trusts, 212

U

- unicast settings, configuring NLB, 71–72
- Universal group scope, 2
- update baselines, 33–36
- Update Baseline Wizard, 33–36
- updating VM images in libraries, 179–180
- /UpdGroup parameter (AdtAdmin), 24
- /UpdForwarder parameter (AdtAdmin), 24
- upgrading AD RMS (Active Directory Rights Management Services), 254–255
- user rights, 3–11
- user roles, VMM (Virtual Machine Manager), 118
- Users container, groups, 9–10

V

- V2V (virtual to virtual) migrations, 168–170
- Validate a Configuration Wizard, 54
- Validate Quorum Configuration test, 62
- validation, certificates, 193–194, 221–223
- validity period, CRLs, 194
- VIP (Virtual IP) templates, automated deployment of NLB, 72–74

- virtual disks
 - creating, 79
 - provisioning options, 80–81
 - resiliency types, 80
- virtual environment delegation, 118–125
 - self-service in VMM, 125
 - VMM, 118–125
- Virtual IP (VIP) templates, automated deployment of NLB, 72–74
- virtualization, servers
 - hosts, 117–130
 - deploying Hyper-V hosts to bare metal, 130
 - host resource optimization, 127–128
 - multi-host libraries, 125–127
 - third-party virtualization platforms, 129–130
 - virtual environment delegation, 118–125
 - managing and maintaining infrastructure, 172–181
 - backup and recovery using DPM, 180–181
 - dynamic and resource optimization, 172–175
 - integration of Operations Manager with VMM and Service Manager, 175–179
 - updating VM images in libraries, 179–180
 - networking, 146–158
 - configuring IP address and MAC address settings, 150–156
 - configuring network optimization, 156–157
 - configuring VMM logical networks, 146–150
 - Windows Server Gateway, 157
 - storage, 159–163
 - Hyper-V clustered storage, 159–162
 - Hyper-V guest storage, 162–163
 - optimization, 163
 - VM movement, 165–170
 - live and storage migration between Hyper-V hosts and clouds, 165–168
 - P2V and V2V, 168–170
 - VMs (virtual machines), 132–144
 - configuring placement rules, 136–140
 - guest resource optimization, 134–137
 - highly available VMs, 132–133
 - VMM templates, 140–144
- Virtual Local Area Networks (VLANs), 146

Virtual Machine Manager

- Virtual Machine Manager. *See* VMM (Virtual Machine Manager)
- Virtual machine queue, 156
- virtual machines. *See* VMs
- virtual switches
 - adding a network site to a logical network, 149
 - configuring in a Hyper-V host, 150
 - extensions, 150
- Virtual Switches dialog box, 150
- virtual to virtual (V2V) migrations, 168–170
- Visual Studio Web Test Monitoring scenario, 25
- VLANs (Virtual Local Area Networks), 146
- VMM (Virtual Machine Manager)
 - automated deployment of NLB, 72–74
 - configuring logical networks, 146–150
 - configuring to move a VM dynamically, 43–44
 - configuring VM placement rules, 136–140
 - Hyper-V networking, 150–151
 - integration with Operations Manager, 39–43, 175–179
 - rights delegation for the private cloud, 19–21
 - self-service, 125
 - storage optimization, 163
 - templates, 140–144
 - update baselines, 33–36
 - virtual environment delegation, 118–125
- VMs (virtual machines)
 - creating networks, 154–156
 - movement, 165–170
 - live and storage migration between Hyper-V hosts and clouds, 165–168
 - P2V and V2V, 168–170
 - server virtualization, 132–144
 - configuring placement rules, 136–140
 - guest resource optimization, 134–137
 - highly available VMs, 132–133
 - VMM templates, 140–144
 - updating images in libraries, 179–180
- VM Template Identity page (Create VM Template Wizard), 140
- VMware vCenter Server, 129, 169–170
- Volume Shadow Copy Service (VSS), 168
- VSS (Volume Shadow Copy Service), 168

W

- wbadmin start systemstaterecovery command, 102
- Web Agents, AD FS, 230
- Web Application Availability Monitoring test, 25
- Web Application Proxy, 230, 239–240
- Web Application Transaction Monitoring, 25
- Weighted Paths DSM setting, 88
- Windows Intune connector (site system role), 16
- Windows Management Instrumentation Query Language (WQL), 24
- Windows Server 2008 mode, 83
- Windows Server Backup, 102–103
- Windows Server Gateway, 157
- witness configuration, 59
- wizards
 - Add Operations Manager, 41–42
 - Add Relying Party Trust, 231
 - Add Revocation Configuration, 206
 - Add Storage Devices, 160–162
 - Add Transform Claim Rule, 233
 - AD FS Federation Server Configuration, 230
 - Certificate Enrollment, 221–222
 - Certificate Trust List, 213–214
 - Configure Cluster Quorum, 60–61
 - Convert Physical Server (P2V), 169–170
 - Create Logical Network, 148–150
 - Create MAC Address Pool, 153–154
 - Create New Protection Group, 106
 - Create Static IP Address Pool, 151–153
 - Create User Role, 17, 119–124
 - Create VM Network, 154–156
 - Create VM Template, 140–144
 - High Availability, 91
 - Import Management Packs, 27
 - Migrate VM, 166
 - New Cluster, 66
 - New Storage Pool, 77
 - New Trust, 211–212
 - New Virtual Disk, 79
 - New Volume, 82–83
 - Operations Manager Setup, 40
 - Protection Agent Installation, 104
 - Publish New Application, 239

Update Baseline, 33–36
Validate a Configuration, 54
workflow, configuration storage in VMM, 160
WQL (Windows Management Instrumentation Query
Language), 24

X

XenServer hosts, 129

This page intentionally left blank

About the author

STEVE SUEHRING is a technical architect with significant hands-on experience in system administration, networking, and computer security. Steve has written on numerous subjects, including Windows, Linux, development, and networking. You can follow him on Twitter at [@stevesuehring](https://twitter.com/stevesuehring).